Guide "Informatique et Libertés" pour l'enseignement supérieur et la recherche

Édition 2009





Guide "Informatique et Libertés" pour l'enseignement supérieur et la recherche

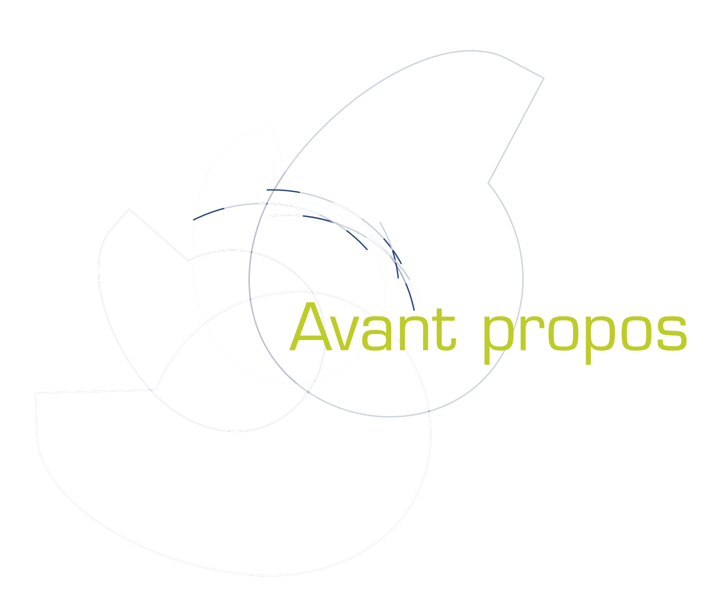
Édition 2009







décembre 2009



Avant propos

L'évolution croissante des technologies de l'information et de la communication et de leurs usages exige que chacun de nous s'approprie les principes du droit fondamental à la protection des données personnelles dans ses deux volets : droits individuels et obligations. C'est à ce prix que nos sociétés innoveront et se développeront dans le respect de la vie privée et des libertés des personnes.

La loi « *Informatique et Libertés* » du 6 janvier 1978, modifiée par la loi du 6 août 2004, définit les principes à respecter lors de la collecte, du traitement et de la conservation des données personnelles. Elle renforce les droits des personnes sur leurs données, prévoit une simplification des formalités administratives déclaratives et précise les pouvoirs de contrôle et de sanction de la CNIL.

Afin de faciliter l'appropriation de ce droit et son application effective au sein des établissements de l'enseignement supérieur, la Conférence des Présidents d'Université (CPU) et la Commission Nationale de l'Informatique et des Libertés (CNIL) ont concrétisé, le 25 janvier 2007, leur partenariat en signant une convention qui vise notamment à promouvoir la nouvelle fonction de « *Correspondant Informatique et Libertés* » *(CIL)*[1].

C'est dans ce cadre que ce guide pratique a été rédigé. Notre souhait est qu'il puisse apporter une réponse concrète à vos questions, lors par exemple, de la mise en place au sein de vos établissements d'un annuaire des anciens diplômés ou d'un espace numérique de travail.

CPU - AMUE - CNIL © 2009

Nous espérons que ce guide permettra ainsi de contribuer au respect et à l'application de la loi et à la diffusion de la culture informatique et libertés au sein de vos établissements. De même, vous pourrez trouver une aide précieuse auprès du correspondant informatique et libertés de votre établissement ou vous rendre sur le site de la CNIL à partir duquel vous pourrez vous abonner à sa lettre d'information (www.cnil.fr) ou consulter la rubrique des actualités.

Bien évidemment, ce guide ne comporte que quelques exemples rencontrés par les Correspondants Informatiques et Libertés nouvellement désignés dans les établissements. Mais nous pensons que par vos remarques éventuelles son contenu ne pourra qu'être enrichi.

La réalisation de ce guide a été rendue possible grâce à un travail d'équipe entre des représentants de la CNIL, de l'Amue, du CRU, de la CPU et de CIL universitaires.

Jean-Pierre FINANCE Président de la CPU	Michel LUSSAULT Président de l'Amue	Alex TÜRK Président de la CNIL

Le guide est mis en ligne sur les sites de la CPU www.cpu.fr, de l'AMUE www.amue.fr et de la CNIL www.cnil.fr

---

[1] Le texte de la loi *"Informatique et Libertés"* utilise l'expression de « *correspondant à la protection des données* ». L'usage a retenu l'expression de « *Correspondant Informatique et Libertés* » (CIL) que nous utiliserons dans le présent guide.

Sommaire général

PARTIE 1

Fiches thématiques

PARTIE 2

Fiches pratiques

CPU - AMUE - CNIL © 2009

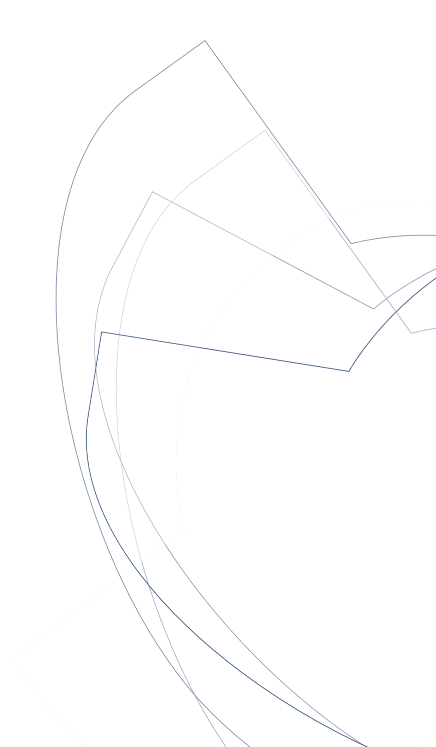
PARTIE 3

Annexes



1

Fiches thématiques



Fiche n°1 Définitions des notions-clés de la loi "Informatique et Libertés"

La loi "*Informatique et Libertés*" du 6 janvier 1978 modifiée est applicable dès lors qu'il existe un traitement automatisé ou un fichier manuel, c'est-à-dire un fichier informatique ou un fichier « papier » contenant des informations personnelles relatives à des personnes physiques.

A noter

Ne sont pas soumis à la loi les « traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles » tels que par exemple les agendas électroniques, les répertoires d'adresses, les sites internet familiaux en accès restreint.

1 Traitement de données à caractère personnel

Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Exemples

Fichiers de gestion des étudiants et des personnels
Annuaire en ligne des anciens diplômés
Espaces numériques de travail

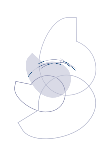
2 Donnée à caractère personnel

Des données sont considérées comme à caractère personnel dès lors qu'elles permettent d'identifier directement ou **indirectement** des personnes physiques (ex. : nom, n° d'immatriculation, n° de téléphone, photographie, éléments biométriques tels que l'empreinte digitale, ADN, numéro d'Identification Nationale Étudiant (INE), ensemble d'informations permettant de discriminer une personne au sein d'une population (certains fichiers statistiques) tels que, par exemple, le lieu de résidence et profession et sexe et age,....).

Il peut en effet s'agir d'informations qui ne sont pas associées au nom d'une personne mais qui permettent aisément de l'identifier et de connaître ses habitudes ou ses goûts.

Exemples

« Le propriétaire du véhicule 3636AB75 est abonné à telle revue » ou encore « l'assuré social 1600530189196 va chez le médecin plus d'une fois par mois ».



A noter

La loi "*Informatique et Libertés*" ne s'applique pas aux personnes morales (ex. : fichier de noms de sociétés). Cependant, si ce fichier d'entreprises contient des noms de personnes physiques (ex : nom du responsable commercial), la loi "*Informatique et Libertés*" est applicable.

3 Responsable du traitement

➢ Est considéré comme le responsable du traitement la personne physique ou morale qui détermine les finalités et les moyens de toute opération (collecte, enregistrement, modification...), appliquée à des données à caractère personnel.

Le responsable du traitement est la personne pour le compte de laquelle est réalisé le traitement. Afin de déterminer l'identité du responsable du traitement, il est possible de faire appel aux critères suivants :

- celui de la « maîtrise d'ouvrage » du traitement : à quoi servira-t-il et comment fonctionnera-t-il ?
- celui de la « mise en œuvre » du traitement : qui décide de s'en servir et qui s'en sert ?

En pratique

Le responsable du traitement sera notamment la personne en charge :

➢ de veiller au respect des principes de la protection des données personnelles ;

➢ d'informer les personnes au sujet de l'existence de leurs droits d'accès, de rectification et d'opposition ;

➢ de désigner, le cas échéant, un Correspondant Informatique et Libertés ;

➢ de procéder à l'accomplissement des formalités auprès de la CNIL sauf en cas de désignation d'un Correspondant Informatique et Libertés[1].

➢ Le responsable du traitement doit être distingué des personnes qui interviennent dans le cadre de sa mise en œuvre du traitement tels que, par exemple, **les sous-traitants**. Le sous-traitant est un exécutant extérieur. Il ne peut agir que sous l'autorité du responsable du traitement et sur instruction de celui-ci. Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la loi. La sous-traitance ne décharge pas le responsable du traitement de sa responsabilité[2].

Exemple

Dans le cas d'un hébergement externe de l'un des sites web de l'université, l'hébergeur est considéré comme le sous-traitant.

[1] Dans le cas de demande d'avis ou de demande d'autorisation, les formalités déclaratives auprès de la CNIL subsistent.
[2] Se reporter à l'annexe 2 : modèle de clause de confidentialité dans le cadre d'un marché ou d'un contrat de sous-traitance.

CPU - AMUE - CNIL © 2009

➢ En dehors du cas où un texte spécifique en dispose autrement, **le responsable du traitement est le représentant légal de l'organisme** (ex. président d'université, directeur d'établissement).

En pratique

Détermination du responsable du traitement dans les Unités Mixtes de Recherche (UMR).

Les responsables du traitement sont d'une part l'université et d'autre part l'organisme de recherche puisque les deux assument la tutelle de l'unité. Cependant afin d'assurer la cohérence des politiques menées, il leur reviendra de définir dans les conventions qui les lient celui d'entre eux qui aura à s'assurer de la bonne application des dispositions "*Informatique et Libertés*" et donc à remplir le rôle de responsable pilote de traitement, unité par unité.

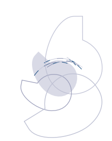
Ainsi, par exemple, la démarche actuelle du CNRS visant à déployer sa politique de sécurité dans chaque laboratoire au niveau régional peut être utile puisqu'elle implique la désignation de la tutelle « pilote » en matière de sécurité des systèmes d'information pour chaque UMR. Selon le CNRS, ce choix devrait figurer dans le contrat quadriennal. Toutefois, dans l'attente de la reconduction de ce contrat, il est proposé que cette désignation soit formalisée dans le cadre d'une convention entre l'université et le CNRS. Cette même démarche pourrait inclure la définition de la tutelle chargée de l'application de la loi "*Informatique et Libertés*" au sein de l'UMR.

Une problématique analogue est susceptible d'apparaître dans le cadre des pôles de recherche et d'enseignement supérieur (PRES) dans la mesure où certains mutualiseront des applications informatiques. Dans ce cas, il faudra explicitement déterminer si la responsabilité du traitement incombe à chaque établissement ou au PRES.

➢ Le responsable du traitement est établi sur le territoire français (installation stable, quelle que soit sa forme juridique, filiale, succursale…) et le traitement est réalisé entièrement sur le territoire de l'Union européenne.

Si le responsable du traitement établi en France transfère des données dans un pays hors de l'Union européenne (ex : hébergeur du site internet, enquêtes réalisées en commun avec des laboratoires de recherche établis hors Union européenne), il devra s'assurer que, dans ce pays, le niveau de protection des données personnelles est considéré comme suffisant. La liste des pays assurant un niveau de protection suffisant est rendue publique sur le site de la CNIL. Dans le cas contraire, le responsable du traitement devra prendre des mesures particulières

Pour toute information complémentaire sur ces questions, consulter le dossier « International » ou le « Guide sur les transferts de données à caractère personnel vers des pays non-membres de l'Union européenne » sur le site internet de la CNIL.



Fiche n°2 Principes de la protection des données personnelles

Les informations que les universités et les établissements de l'enseignement supérieur traitent informatiquement pour remplir leurs missions de service public doivent être protégées parce qu'elles relèvent de la vie privée et parce que leur divulgation est susceptible de porter atteinte aux droits et libertés des personnes concernées.

La loi "*Informatique et Libertés*" a défini les principes à respecter lors de la collecte, du traitement et de la conservation de ces données. La loi prévoit également un certain nombre de droits pour les personnes dont les données personnelles ont été recueillies.

Le respect, par les universités et les établissements de l'enseignement supérieur, des règles de protection des données à caractère personnel est un facteur de transparence et de confiance à l'égard des personnes (étudiants, personnels). C'est aussi un gage de sécurité juridique pour les présidents d'université et directeurs d'établissement qui, responsables des fichiers mis en œuvre, doivent veiller à ce que la finalité de chaque traitement informatique et les éventuelles transmissions d'informations soient clairement définies, les dispositifs de sécurité informatique précisément déterminés et les mesures d'information des usagers appliquées.

1 Le principe de finalité : une utilisation encadrée des fichiers

Les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime, correspondant aux missions de l'établissement, responsable du traitement. C'est au président d'université ou au directeur d'établissement qu'il appartient de fixer la finalité des traitements mis en œuvre pour le compte de son université ou de son établissement et de la faire respecter.

Tout détournement de finalité est passible de sanctions pénales.

Exemple

Le fichier de gestion administrative et pédagogique des étudiants ne peut être utilisé à des fins commerciales ou politiques.

2 Le principe de proportionnalité

Seules doivent être enregistrées les informations pertinentes et nécessaires pour assurer la gestion des services universitaires.

Exemple

Demander le revenu des parents de l'étudiant pour recevoir la « newsletter » de l'établissement n'est ni pertinent ni nécessaire au regard de la finalité poursuivie par le traitement.

CPU - AMUE - CNIL © 2009

3 Le principe de durée limitée de conservation des données : le droit à l'oubli

Les informations ne peuvent être conservées de façon indéfinie dans les fichiers informatiques. Une durée de conservation doit être établie en fonction de la finalité de chaque fichier.

Exemples

Les informations collectées dans le cadre de l'organisation d'un examen ou d'un concours sont conservées pour la durée de la session de l'examen ou du concours.

Une mise à jour du fichier des abonnés à la « newsletter » (lettre d'information électronique) de l'université est effectuée chaque année, avec une proposition de réinscription adressée aux étudiants. Les données sont supprimées au plus tard 6 mois après la proposition de réinscription restée sans réponse.

Au-delà, les données peuvent être archivées, sur un support distinct[1].

4 Le principe de sécurité et de confidentialité

Le président d'université ou le directeur d'établissement, en tant que responsable du traitement, est astreint à une obligation de sécurité : il doit faire prendre les mesures nécessaires pour garantir la confidentialité des données et éviter leur divulgation.

➢ Les données contenues dans les fichiers ne peuvent être consultées que par les services habilités à y accéder en raison de leurs fonctions.

Exemple

Veiller à ce que chaque utilisateur ait un mot de passe individuel régulièrement changé et que les droits d'accès soient précisément définis en fonction des besoins réels.

➢ Le responsable du traitement doit prendre toutes mesures pour empêcher que les données soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Exemple

S'il est fait appel à un prestataire externe, des garanties contractuelles doivent être envisagées[2].

➢ Les mesures de sécurité, tant physique que logique, doivent être prises.

---

1 La durée de conservation déclarée dans le dossier de formalité adressé à la CNIL ou dans le registre du CIL doit correspondre à la période durant laquelle les données restent accessibles ou consultables directement par le personnel, par opposition avec la période d'archivage des données pendant laquelle celles-ci ne sont plus destinées à être utilisées à des fins de gestion et sont de ce fait, conservées sur un support distinct au sein d'un service d'archives. Se reporter à l'instruction ministérielle sur l'archivage (référence : DAF DPACI/RES/2005/003 du 22 février 2005).

2 Voir annexe 2 : modèle de clause de confidentialité dans le cadre d'un marché ou d'un contrat de sous-traitance.



Exemples

Protection anti-incendie, copies de sauvegarde, installation de logiciel antivirus, changement fréquent des mots de passe alphanumériques d'un minimum de 8 caractères.

➢ Les mesures de sécurité doivent être adaptées à la nature des données et aux risques présentés par le traitement.

Exemples

Authentification forte pour l'accès aux résultats d'examen, chiffrement des coordonnées bancaires transitant sur internet.

5 Le principe du respect du droit des personnes

5.1 Informer les intéressés

Lors de l'informatisation de tel ou tel service, ou lorsque des données sont recueillies par exemple par voie de questionnaires, les usagers concernés et le personnel de l'organisme doivent être informés de la finalité du traitement, du caractère obligatoire ou facultatif du recueil, des destinataires des données et des modalités d'exercice des droits qui leur sont ouverts au titre de la loi "*Informatique et Libertés*" : droit d'accès et de rectification mais aussi, droit de s'opposer, sous certaines conditions, à l'utilisation de leurs données.

Cette information doit être diffusée, par exemple, au moyen d'affiches apposées dans les services recevant du public et portée sur les formulaires établis par l'établissement, ainsi que sur les courriers adressés aux personnes dont les données sont collectées.

En pratique

Des modèles de mentions d'information sont disponibles en annexe 2.

5.2 Les droits d'accès et de rectification

Toute personne (étudiant, personnel) peut demander communication de toutes les informations la concernant contenues dans un fichier détenu par l'établissement et a le droit de faire rectifier ou supprimer les informations erronées.

5.3 Le droit d'opposition

Toute personne a le droit de s'opposer, pour des motifs légitimes, à ce que des données la concernant soient enregistrées dans un fichier informatique, sauf si celui-ci présente un caractère obligatoire.

Exemple

Le fichier de gestion administrative des étudiants ou encore le fichier de gestion de prêts de livres de la bibliothèque présentent un caractère obligatoire à l'inverse de l'annuaire des anciens étudiants.

CPU - AMUE - CNIL © 2009

Fiche n°3 Rôle de la CNIL pour défendre ces principes

La Commission nationale de l'informatique et des libertés, autorité administrative indépendante chargée d'assurer le respect des dispositions de la loi "*Informatique et Libertés*"[1] a, à cet égard, deux missions principales :

- informer les personnes concernées de leurs droits et les responsables de traitements de leurs obligations ;
- veiller à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la loi "*Informatique et Libertés*".

1 Le contrôle de la conformité à la loi des projets de fichiers et traitements

C'est au titre de ses missions que la CNIL vérifie, lors de l'instruction des déclarations de fichiers qui lui sont adressées, que les caractéristiques des traitements concernés sont bien conformes à la loi et autorise la mise en œuvre des traitements qui, aux termes de la loi, nécessitent une attention particulière du fait de leur contenu, de leur finalité ou de leur structure.

C'est également à ce titre que la Commission peut simplifier les formalités déclaratives, voire exonérer de déclaration certains fichiers.

Afin de présenter de manière synthétique les différentes formalités à respecter en la matière, le Guide fait figurer en annexe 1 un mode d'emploi détaillant les procédures existantes.

La modification de la loi introduite en 2004 a également prévu une autre source de simplification des formalités préalables dès lors qu'un organisme a désigné un Correspondant Informatique et Libertés (se reporter à la fiche n°4 du guide).

Afin de promouvoir cette nouvelle fonction de Correspondant Informatique et Libertés (CIL) au sein de l'enseignement supérieur, la CNIL et la CPU ont signé en 2007 une convention de partenariat.

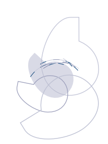
2 Le rôle de conseil et d'information

De même, la CNIL conseille et renseigne les personnes et les organismes qui envisagent de mettre en œuvre des fichiers informatiques, que ce soit au téléphone, par courrier ou par ses publications. Elle s'est dotée d'un « Service d'Orientation et de Renseignement du Public » (SORP) afin d'apporter une réponse rapide aux requêtes des particuliers comme des professionnels relative à l'application de la loi.

Lorsque de nouvelles technologies apparaissent, la CNIL procède à des études, élabore en concertation avec les milieux concernés des recommandations, le cas échéant propose des mesures législatives. Ces activités peuvent également être menées avec ses homologues en particulier européens.

---

1 Les textes cités en référence (la loi "*Informatique et Libertés*", normes simplifiées applicables, délibérations et guides) sont disponibles le site web de la CNIL : http://www.cnil.fr.



3 L'instruction des plaintes

La CNIL reçoit les plaintes concernant le non-respect de la loi. Selon la nature et l'importance des manquements, elle procède au règlement des plaintes soit par voie amiable, soit par la mise en œuvre de son pouvoir de sanction, soit en dénonçant les faits au procureur.

4 Le pouvoir de vérification sur place

La CNIL dispose d'un pouvoir de contrôle qui permet à ses membres et ses agents d'accéder à tous les locaux professionnels. Sur place, ses membres et agents peuvent demander communication de tout document nécessaire et en prendre copie, recueillir tout renseignement utile et accéder aux programmes informatiques et aux données.

5 Le pouvoir de sanction

Au titre de son pouvoir de sanction, la CNIL peut :

- adresser des avertissements et des mises en demeure de faire cesser un manquement à la loi ;
- prononcer une injonction de cesser le traitement ou un retrait de l'autorisation et, en cas d'urgence, décider l'interruption du traitement ou le verrouillage des données ;
- prononcer des sanctions pécuniaires pouvant aller jusqu'à 300 000 € en cas de réitération ;
- dénoncer au parquet les infractions à la loi dont elle a connaissance.

6 La CNIL dans le monde

De manière générale, la CNIL peut être associée, à la demande du premier ministre, aux négociations internationales dans son domaine de compétence.

Elle exerce par ailleurs des missions particulières liées à la mise en œuvre d'instruments européens et développe une politique de coopération en direction des pays non encore dotés d'une législation.

Au niveau européen

L'Union européenne a adopté le 24 octobre 1995 une directive destinée à assurer une protection équivalente en son sein quelque soit le lieu où sont opérés les traitements de données à caractère personnel au moyen d'une harmonisation des législations des Etats membres (27 à ce jour auxquels s'ajoutent les pays de l'Espace Economique Européen (Islande, Liechtenstein, Norvège). Cette harmonisation comporte également une approche commune visant la protection des personnes dont les données sont susceptibles d'être transférées vers des pays hors Union européenne.

Les autorités indépendantes de ces pays se réunissent régulièrement à Bruxelles pour conseiller la Commission européenne sur ses initiatives législatives et pour harmoniser leurs interprétations des textes et leurs pratiques ou recommandations destinées aux concepteurs et aux utilisateurs des technologies de l'information.

CPU - AMUE - CNIL © 2009

Ces « CNIL » européennes réunies au sein du « groupe de l'article 29 », par référence à l'article de la directive qui l'institue, se prononcent par des avis ou recommandations qui sont rendus publics[2]. Dans ce cadre, elles déterminent également des programmes de contrôle communs notamment de nature sectorielle.

Au niveau international

La CNIL est amenée à coopérer également, notamment dans le cadre de règlement de plaintes, avec les autorités de même nature instituées dans d'autres pays européens non membres de l'Union tels que la Principauté d'Andorre, les îles anglo-normandes, la Croatie, Gibraltar, l'ex République yougoslave de Macédoine, Monaco et la Suisse.

De même elle coopère avec des autorités non européennes établies sur d'autres continents dans des pays tels que le Canada, l'Argentine, l'Australie, la Nouvelle Zélande, et le Burkina Faso dotés d'une loi et d'une autorité indépendante de contrôle.

Avec d'autres pays la coopération est plus limitée lorsque ceux ci ont fait le choix d'adopter une législation applicable au seul secteur public ou à certaines activités du secteur privé (USA, Corée du Sud par exemple).

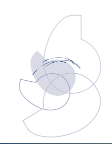
Etant donné l'accélération des transferts de données sur le plan mondial et le faible nombre de pays dotés d'une loi « informatique et libertés » notamment au Sud (4/5 des pays au monde ne sont pas encore dotés d'une telle législation), l'ensemble des « CNIL » ont lancé un appel en 2005 en faveur d'un instrument contraignant de portée mondiale (déclaration de Montreux).

Dans l'attente d'un tel instrument, la CNIL apporte son expertise notamment auprès de pays francophones souhaitant mettre en place une législation « informatique et libertés» et a suscité en 2007 la création d'une association des « CNIL » francophones. Une politique analogue est mise en œuvre par l'autorité espagnole en direction des pays d'Amérique latine.

Enfin, lors de la Conférence internationale de novembre 2006, le président de la CNIL a proposé à ses collègues une initiative dite « de Londres ». Il s'agit de faire face au double défi actuel qui fragilise et menace le droit à la vie privée et à la protection des données, qui est d'une part l'accélération et la mondialisation des nouvelles technologies, et d'autre part la vague normative liée aux nouvelles législations de lutte antiterroriste. Le programme d'activités communes adopté vise le renforcement des capacités d'expertise, de prospective et d'intervention dans le domaine des nouvelles technologies, l'évaluation des missions et pouvoirs en particulier en matière d'investigation, l'intensification de la sensibilisation des acteurs, notamment des jeunes et des élus nationaux et locaux, la coordination de la communication.

---

2 http://ec.europa.eu/justice_home/fsj/privacy/index_fr.htm.



Fiche n°4 Correspondant Informatique et Libertés

Institué à l'occasion de la refonte de la loi "*Informatique et Libertés*", le Correspondant Informatique et Libertés est un acteur et un relais incontournable de la culture "*Informatique et Libertés*".

➢ Qu'est-ce que le Correspondant Informatique et Libertés ?

Le Correspondant Informatique et Libertés (CIL) a vocation à être un interlocuteur spécialisé en matière de protection de données à caractère personnel, tant pour le président d'université ou directeur d'établissement, que dans les rapports de ce dernier avec la CNIL. Le CIL occupe ainsi une place centrale dans le développement maîtrisé des nouvelles technologies de l'information et de la communication.

Cette fonction existe déjà chez plusieurs de nos voisins européens (Allemagne, Pays-Bas, Suède, Luxembourg).

➢ Pourquoi désigner un Correspondant Informatique et Libertés ?

La fonction de correspondant répond à un double objectif.

- Elle emporte un allègement considérable des formalités auprès de la CNIL. Sa désignation permet en effet d'être exonéré de l'obligation de déclaration préalable des traitements ordinaires et courants. Seuls les traitements identifiés comme sensibles dans la loi demeurent soumis à autorisations et continuent à faire l'objet de formalités.

- Le Correspondant Informatique et Libertés apporte une aide précieuse au président d'université ou directeur d'établissement. Il contribue à une meilleure application de la loi et réduit ainsi les risques juridiques pesant sur l'organisme concerné.

Il a un rôle de conseil, de veille et d'alerte en matière de déploiement des projets informatiques au sein de l'organisme. Il joue également un rôle essentiel dans la formation et la sensibilisation des personnels de l'établissement aux principes "*Informatique et Libertés*".

➢ Quelles sont les compétences requises pour être Correspondant Informatique et Libertés ?

Le CIL peut être un employé de l'établissement ou une personne externe (comme par exemple, un consultant, un avocat…). La loi a fixé des seuils pour déterminer les cas dans lesquels il est possible de choisir un CIL interne ou externe à l'établissement.

Ainsi, il existe une liberté de choix lorsque moins de 50 personnes sont chargées de la mise en œuvre des traitements ou qui y ont directement accès. Le choix est limité lorsque plus de 50 personnes sont chargées de la mise en œuvre des traitements ou y ont directement accès.

CPU - AMUE - CNIL © 2009

En pratique, pour connaître le seuil applicable, il convient de déterminer le nombre de personnels qui sont chargés :

- du développement et de la maintenance des applications tel que, par exemple, le service informatique ;
- de la saisie des données ou de la consultation (ex. : service juridique, comptable, ou des ressources humaines).

Le nombre de 50 personnes est apprécié au regard de l'ensemble des applications informatiques mises en œuvre par l'université ou l'établissement.

Exemple

Il est possible de désigner un CIL pour plusieurs établissements dans lesquels plus de 50 personnes sont chargées de la mise en œuvre des traitements ou y ont directement accès. Dans ce cas, le CIL doit être une personne mandatée par un organisme représentant les universités. Cette désignation pourrait ainsi être faite au niveau d'un Pôle de Recherche et d'Enseignement Supérieur (PRES).

La plupart des correspondants ont une formation informatique mais ce n'est pas une obligation légale. L'important est qu'il puisse, si nécessaire, bénéficier d'une formation tant technique que juridique, qui soit adaptée à la taille de l'établissement. S'il n'est pas prévu d'agrément par la CNIL, celle-ci doit néanmoins enregistrer la désignation et notifier celle-ci au responsable du traitement.

Quel que soit le choix fait, l'essentiel est qu'il y ait une très bonne collaboration entre le CIL, le RSSI (Responsable de la Sécurité des Systèmes d'Information), le CRI (Centre de Ressources Informatiques) et le service juridique de l'établissement.

Enfin, pour s'acquitter de sa tâche, le Correspondant Informatique et Libertés doit disposer de la liberté d'action et des moyens qui lui permettront de recommander des solutions organisationnelles ou techniques adaptées. Il doit pouvoir exercer pleinement ses missions, en dehors de toute pression, et jouer son rôle auprès du responsable du traitement.

➢ Qui peut désigner un Correspondant Informatique et Libertés ?

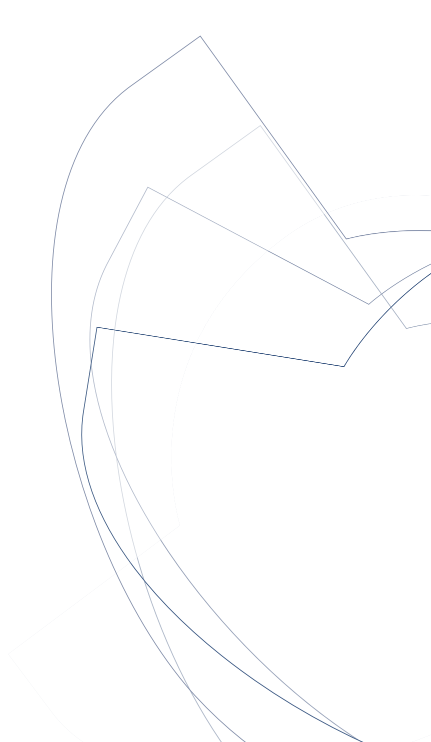
Il appartient au responsable du traitement d'exercer un choix.

Ainsi, dans le secteur public, les collectivités territoriales, les administrations de l'Etat, les établissements publics etc. peuvent faire le choix de désigner un correspondant. Il en va de même des PME, des entreprises multinationales, des associations... La désignation d'un correspondant est facultative et traduit l'engagement du responsable du traitement à respecter les dispositions légales.

En pratique

Pour toute information complémentaire sur le correspondant, sa désignation et ses missions, consulter le dossier « Correspondant » ou le « Guide du Correspondant Informatique et Libertés » sur le site internet de la CNIL. Vous pouvez également contacter le service de la CNIL en charge des correspondants.

2 Fiches pratiques



Fiche n°5 Mise en place d'un annuaire des diplômés

De quoi s'agit-il ?

La mise en place par une association d'anciens étudiants ou par l'établissement lui-même d'un annuaire des diplômés est une pratique courante.

En quoi mes libertés sont-elles concernées ?

La création d'un annuaire d'anciens diplômés peut en pratique soulever des difficultés au regard des principes "Informatique et Libertés" s'agissant plus particulièrement des conditions dans lesquelles il a été constitué et des modalités de sa diffusion (papier, internet).

En effet, la divulgation sur internet du nom et de l'adresse personnelle des anciens étudiants sans qu'ils en aient été préalablement informés et en mesure de s'y opposer peut comporter un risque pour leur vie privée. Ces informations peuvent, par exemple, être collectées à leur insu notamment à des fins de sollicitations commerciales.

Que faire ?

Tout nouveau diplômé se voit proposer par l'établissement un formulaire d'inscription à l'annuaire. Celui-ci devra notamment préciser la finalité de la collecte, à savoir la mise en place d'un annuaire des diplômés de l'établissement, son caractère facultatif, les destinataires des données et les modalités d'exercice des droits d'accès, de rectification et d'opposition aux données.

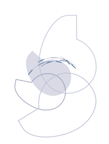
Dans l'hypothèse où l'annuaire serait accessible sur internet, les anciens élèves doivent en être préalablement informés et mis en mesure de s'opposer à la diffusion de leurs coordonnées. Il est recommandé que l'accès à l'annuaire via internet soit strictement réservé aux anciens étudiants (exemple : attribution de code d'accès).

Il est également souhaitable que le formulaire d'inscription puisse permettre au diplômé d'indiquer les informations qu'il souhaite ne pas voir diffuser (ex : son adresse personnelle) tant sur la version web que sur la version papier de l'annuaire. Ces données ne restent alors accessibles qu'au service chargé de la tenue de l'annuaire.

Un ancien diplômé qui aura été recontacté individuellement (lors d'un événement professionnel par exemple) pourra se voir proposer le formulaire d'inscription à l'annuaire.

Chaque année, un courrier électronique ou postal doit être envoyé à chacun des diplômés inscrits sur l'annuaire, leur rappelant les modalités de mise à jour de leurs données personnelles, ainsi que celles de désinscription.

Si ce courrier revient en NPAI (*N'habite Plus A l'Adresse Indiquée*), toutes les données relatives à ce diplômé sont supprimées.



L'autre cas de suppression des données correspond à une désinscription explicite de la part du diplômé.
Il est important également de veiller à insérer une mention légale sur l'annuaire qui précise qu'en aucun cas les données qu'il contient ne peuvent être exploitées à des fins commerciales ou politiques sauf indication explicite en sens contraire de la personne concernée.

En pratique

Les associations d'anciens élèves

L'université ou l'établissement peut communiquer la liste de ses anciens diplômés à ces associations dès lors que les intéressés ont, d'une part, été préalablement informés de ladite transmission les concernant et ont, d'autre part, eu la possibilité de s'y opposer.
Par ailleurs, l'établissement peut, par voie d'affichage et plus particulièrement lors de la publication des résultats, informer les diplômés de l'existence d'associations d'anciens élèves et des modalités d'inscription via par exemple le site web de l'association.

CPU - AMUE - CNIL © 2009

Fiche n°6 Diffusion des résultats d'examen et des notes sur internet



De quoi s'agit-il ?

Comme le précise une circulaire ministérielle, les résultats des examens sont portés à la connaissance des étudiants par voie d'affichage[1]. Traditionnellement, cette proclamation des résultats est réalisée par le biais d'un affichage dans les locaux de l'université ou de l'établissement. Cette publicité ne s'applique pas aux notes obtenues qui sont communiquées individuellement à chaque étudiant.

Il est désormais fréquent que les universités permettent à leurs étudiants d'accéder à leurs résultats d'examen et à leurs notes via internet.



En quoi mes libertés sont-elles concernées ?

La diffusion des résultats d'examen et des notes des étudiants via internet est susceptible de porter atteinte à la vie privée des personnes compte tenu des caractéristiques propres au réseau internet qui est par principe un réseau ouvert au public. En effet, ces informations sont susceptibles d'être captées et utilisées par des tiers dès lors qu'elles sont diffusées sur le réseau.



Que faire ?

1. Informer les étudiants de la diffusion sur internet

S'agissant de la publicité des résultats d'examen (admis, ajourné) sur internet et en l'absence de règles définissant les modalités de diffusion des résultats des examens, il est recommandé que les étudiants aient été préalablement informés d'une telle diffusion et mis en mesure de s'y opposer. Cette information peut, par exemple, être prévue sur le dossier d'inscription de l'étudiant.

S'agissant de la mise en ligne des notes d'examen, chaque personne concernée doit disposer d'un code d'accès et d'un mot de passe (accès restreint) pour les obtenir. L'accès aux notes, qui sont des données personnelles, est en effet strictement personnel. Le plus souvent, cet accès est réalisé via le compte ENT de l'étudiant.

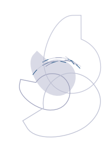
2. Déclarer auprès de la CNIL

L'accès aux résultats d'examen et aux notes via internet par le biais d'identifiants de connexion doit être considéré comme un téléservice de l'administration électronique. Sa mise en œuvre est par conséquent soumise à avis préalable de la CNIL. Si cet accès est envisagé dans le cadre d'un ENT, il peut être déclaré sous une forme simplifiée à condition que le dispositif ENT respecte le cadre fixé par l'arrêté du 30 novembre 2006[2].

---

1 Circulaire ministérielle n°2000-033 du 1er mars 2000.

2 Cf. Annexe 1 : Comment déclarer ? et Fiche 12 du guide sur les Espaces Numériques de Travail.



Fiche n°7 Utilisation de la photographie d'une personne

De quoi s'agit-il ?

L'utilisation de la photographie d'une personne ou d'un groupe de personnes est devenue une pratique courante au sein de l'enseignement supérieur. Elle est, par exemple, apposée sur la carte de l'étudiant, sur des fiches d'inscription à des travaux dirigés et/ou pratiques, sur des articles publiés dans une revue ou un journal d'école ou de laboratoire, sur un site internet, sur un répertoire de chercheurs ou encore sur un trombinoscope.

En quoi mes libertés sont-elles concernées ?

L'image d'une personne est considérée comme un attribut de sa personnalité ou encore comme un élément de l'intimité de sa vie privée et elle est protégée au titre du droit au respect de la vie privée. Son utilisation en est dès lors strictement encadrée ; en effet, toute personne dispose sur son image et sur l'utilisation qui en est faite, d'un droit exclusif et peut s'opposer à sa reproduction et diffusion dès lors qu'elle n'y a pas préalablement consenti.

Que faire ?

1. Recueillir l'accord des personnes photographiées

La prise de photographies et leur diffusion doivent s'effectuer dans le respect des règles relatives au droit à l'image.

Toute personne pouvant s'opposer à la reproduction de son image, sur quelque support que ce soit (diffusion de son image sur un intranet, sur internet, etc.), la prise d'une photographie et sa diffusion doivent faire l'objet d'un accord écrit de la personne concernée si elle est majeure ou de ses représentants légaux s'il s'agit d'un étudiant mineur.

Il appartient donc au responsable d'obtenir toutes les autorisations utiles préalablement à l'utilisation de photographies.

Pour autant, lorsque la capture de l'image d'une personne a été accomplie au vu et au su de l'intéressée sans qu'elle s'y soit opposée alors qu'elle était en mesure de le faire, son consentement est présumé.

2. Déclarer auprès de la CNIL

Dès lors qu'elle se rapporte à une personne identifiée ou identifiable, l'image d'une personne est une donnée à caractère personnel. Le traitement informatique de cette donnée (numérisation, diffusion à partir d'un site web, etc.) doit s'effectuer dans le respect de la loi "Informatique et Libertés" et donc ainsi être déclaré auprès de la CNIL sauf en cas de désignation d'un Correspondant Informatique et Libertés.

CPU - AMUE - CNIL © 2009

Fiche n°8 Enquêtes statistiques portant sur le devenir professionnel et le suivi de cohortes d'étudiants

De quoi s'agit-il ?

La mise en place des indicateurs de performances dans le cadre de la LOLF et la nécessité d'adapter au mieux l'offre de formation contribuent au développement d'enquêtes de suivi de cohorte d'étudiants. En effet, suivre le parcours des étudiants dans le cadre d'un suivi de cohorte est l'occasion d'observer dans la durée le devenir des diplômés et de mieux comprendre leur orientation.

Le plus souvent, les informations à caractère personnel nécessaires à la réalisation de ce suivi seront extraites de la base de gestion des étudiants et peuvent être complétées par des enquêtes auprès d'étudiants (ex. : connaître pour chaque diplômé, sortant de l'Université pour entrer sur le marché du travail, son devenir professionnel 18 mois et 3 ans après l'obtention du diplôme).

Les informations recueillies sont ensuite utilisées et analysées dans un but statistique.

Dans la plupart des cas, ces études sont menées par les Observatoires de la Vie Étudiante, structures chargées, au sein des universités d'élaborer, des outils d'analyse et d'aide à la décision.

En quoi mes libertés sont-elles concernées ?

Si la légitimité de ce type d'études ne saurait être remise en question, elles doivent cependant être réalisées dans le respect des droits des personnes (information préalable, droit d'accès, de rectification et d'opposition).

En outre, le risque d'une exploitation des données à des fins autres que celle d'un suivi de cohorte étant toujours possible, une attention particulière doit être apportée aux mesures prises pour assurer la sécurité et la confidentialité de ces traitements et notamment garantir l'anonymat des réponses.

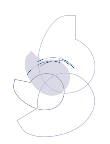
Que faire ?

Les responsables de ces études doivent veiller à la mise en place des mesures suivantes :

➢ une information préalable des étudiants relative à la mise en place de ce type d'études au sein de l'établissement doit être prévue. Celle-ci peut par exemple être réalisée au moment de l'inscription de l'étudiant ;

➢ le questionnaire d'enquête adressé aux (anciens) étudiants doit :
  - rappeler les mentions de la loi "Informatique et Libertés" ; celles-ci doivent également figurer sur la lettre d'accompagnement ;
  - indiquer qu'il reste facultatif et est confidentiel ;
  - comporter des questions qui restent pertinentes et adaptées au regard de la finalité de l'enquête ;

➢ une fois l'enquête considérée comme terminée, les informations personnelles détenues par le responsable de l'enquête doivent être détruites ou archivées; seuls les résultats statistiques peuvent être conservés ;



➢ un pilotage rigoureux et officiel de cette étude est assuré par exemple par le vice-président CEVU (Conseil des Études et de la Vie Universitaire) ;
➢ les statistiques nécessaires seront réalisées par des personnes habilitées à utiliser de la base de gestion des étudiants ;
➢ une information sur l'enquête devra être présentée régulièrement « au fil de l'eau » : journal de l'établissement, présentation des résultats lors des « journées scolarité », des réunions d'accueil des étudiants…

Se reporter à l'annexe 1 « Mode d'emploi : comment déclarer ? » qui précise les cas dans lesquels ces traitements relèvent du régime de la déclaration normale ou de la demande d'autorisation.

CPU - AMUE - CNIL © 2009

Fiche n°9

Études menées au sein de l'enseignement supérieur afin de mesurer la diversité des origines des étudiants et les pratiques discriminatoires



De quoi s'agit-il ?

Les universités peuvent être intéressées à étudier la diversité des étudiants qu'elles accueillent, et notamment la diversité géographique, religieuse et sociale. De même, ces études peuvent avoir pour objectif de constater le niveau d'impact des « origines » sur les parcours des personnes inscrites dans l'enseignement supérieur afin d'évaluer la présence éventuelle de pratiques discriminatoires.



En quoi mes libertés sont-elles concernées ?

Ce type d'étude peut entraîner la collecte et l'exploitation des données dites sensibles à savoir des « ***données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions*** *politiques, philosophiques ou* ***religieuses*** *ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci » (art.8 de la loi "Informatique et Libertés").*

Ces données touchent ainsi à l'essence même de ce qui fait notre identité, à la façon dont on se perçoit et dont on est perçu par les autres. C'est pourquoi leur traitement fait l'objet d'une attention toute particulière.



Que faire ?

1. Déterminer une méthodologie d'étude

Trois procédés peuvent notamment être envisagés afin de mesurer la diversité des origines ou les pratiques discriminatoires :

1.1 Utiliser des données sur la nationalité

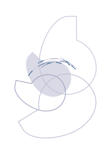
Faisant partie de l'état civil, cette donnée n'est pas considérée comme sensible. Ainsi, elle peut être utilisée afin d'établir des statistiques par pays d'origine des étudiants inscrits à l'université[1].

1.2 Utiliser les noms et les prénoms

La CNIL estime que l'analyse des noms et prénoms, aux fins de classement dans des catégories «ethno-raciales », n'est pas pertinente en raison du manque de fiabilité de cette méthode et du risque de stigmatisation qui pourrait en découler.

En revanche, elle considère que le recours au prénom ainsi que, le cas échéant au nom de famille, pour détecter d'éventuelles pratiques discriminatoires dans le parcours universitaire, à l'exclusion de tout classement dans des catégories « ethno-raciales »,

[1] Il est à noter la mise en place en 2003 par le Ministère de la jeunesse, de l'éducation nationale et de la recherche d'un traitement d'informations individuelles dénommé « Système d'Information sur le Suivi de l'Étudiant (SISE) » qui inclut notamment la nationalité. Cette donnée donne lieu à la production de tableaux statistiques anonymes permettant de connaître la répartition des effectifs des étudiants selon leur nationalité.



peut constituer un indicateur intéressant sur le plan statistique dès lors que les conditions suivantes sont réunies :

➢ l'analyse de ce seul critère ne saurait être suffisante pour apprécier la discrimination ; il convient de procéder à une analyse réellement objective (multi-critères) des parcours ou des trajectoires de vie prenant en compte l'ensemble des autres facteurs discriminants (ex : sexe, âge, lieu de résidence, catégorie socio-professionnelle…) ou susceptibles d'expliquer la différence de parcours (ex : diplômes, compétences, ancienneté et expérience professionnelle …) ;

➢ le recours au prénom et au nom de famille peut constituer un repère pour étudier les trajectoires de populations issues de l'immigration, quand il n'existe pas d'autre source disponible ;

➢ de telles études doivent être conduites selon une méthodologie rigoureuse :
- l'analyse des noms et des prénoms doit seulement permettre un classement de ces données en catégories « potentiellement discriminant » / « non-discriminant » ;
- les fichiers de gestion (fichiers de personnel, fichiers d'élèves, d'étudiants, …), les annuaires professionnels et d'anciens élèves ne peuvent être utilisés qu'à des fins statistiques de suivi des trajectoires et d'évaluation des politiques de lutte contre les discriminations ;
- des mesures doivent être prises pour assurer la confidentialité des données traitées, garantir l'anonymat des résultats et informer les personnes concernées de la finalité de l'étude, des conditions de sa réalisation et de leur droit de s'opposer au traitement de leurs données.

Exemple

Afin de repérer les étudiants concernés par l'étude, un observatoire régional s'est limité à établir la liste des prénoms potentiellement discriminant sans retourner aux noms des personnes (procédure initialement envisagée pour vérifier les prénoms incertains). Cet observatoire disposait donc d'une liste qui comportait pour chaque prénom l'indication du sexe, de la catégorie socio-professionnelle du chef de famille, de la série du bac, de la précocité au baccalauréat. Ce fichier était ainsi complètement anonyme et ne relevait plus des dispositions de la loi "Informatique et Libertés".

1.3 Mesurer la diversité par le biais d'enquêtes sur le « ressenti » des discriminations

Ces enquêtes doivent être basées sur le volontariat et l'auto-déclaration. Les enquêtes anonymes pourraient, pour certaines, reposer sur la constitution de panels permettant ainsi de suivre les trajectoires des personnes.

2. Informer les personnes concernées

L'information des personnes est essentielle. Chaque responsable d'établissement se doit d'informer les étudiants de leurs droits au regard de la loi "Informatique et Libertés".

En pratique

Le dossier d'inscription dans les universités et les établissements d'enseignement supérieur doit comporter une mention très explicite relatives aux études statistiques menées au sein des ces universités et établissements.

CPU - AMUE - CNIL © 2009

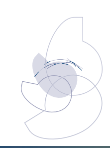
3. Déclarer auprès de la CNIL

Si le traitement est susceptible de faire apparaître les origines supposées ou réelles des étudiants ou leur confession de façon directement ou indirectement nominative, il est nécessaire de procéder à une déclaration de ce traitement à la CNIL.

Se reporter à l'annexe 1 « Mode d'emploi : comment déclarer ? » qui précise les cas dans lesquels ces traitements relèvent du régime de la déclaration normale ou de la demande d'autorisation.
Si les enquêtes sont anonymes, celles-ci ne sont pas soumises à la loi "Informatique et Libertés" et n'ont pas à être déclarées à la CNIL.

En pratique

Pour en savoir plus, consulter le rapport du 15 mai 2007 de la CNIL « Mesure de la diversité et protection des données personnelles » ainsi que « Les dix recommandations de la CNIL ».



Fiche n°10 Mise à disposition ou accès à des ressources numériques via des dispositifs de « fédération d'identités »

A noter

Cette fiche s'adresse plus particulièrement au service informatique de l'université ou de l'établissement.

De quoi s'agit-il ?

Certains établissements de l'enseignement supérieur ou universités ont choisi d'utiliser des mécanismes dits de « fédération d'identités[1] » afin d'assurer auprès de leurs étudiants, chercheurs et personnels, la mise à disposition ou l'accès simplifié à des ressources numériques qui leur sont réservées par des entités publiques ou privées[2]. Il pourra s'agir de l'accès à des cours en ligne, à des services ou produits aux tarifs préférentiels pour des étudiants ou à de la documentation numérique.

En ce qu'elle permet de certifier des qualités déterminées de telle ou telle personne (« Mme X est bien étudiante en licence de droit » si cette information est requise pour accéder au service ou « M.Y est bien étudiant à l'université U » si cette information est suffisante), le déploiement d'une fédération d'identités sécurise l'accès à ces ressources.

Il simplifie également l'accès ou la mise à disposition de ces ressources dans la mesure où il sera possible de partager une application entre plusieurs partenaires sans devoir réenregistrer tous les nouveaux utilisateurs de cette application ou encore de contrôler la diffusion d'informations concernant ses utilisateurs à des partenaires extérieurs.

Exemples

- Un étudiant accède à une plate-forme d'enseignement à distance sur le thème de la biologie. Cette dernière peut interroger son université d'appartenance pour connaître sa filière d'enseignement. S'il s'agit de la biologie, l'étudiant est autorisé à accéder aux ressources de cette plate-forme, sinon l'accès lui est refusé.
- Des éditeurs de logiciels souhaitant proposer des tarifs très bas aux étudiants doivent s'assurer de la qualité de l'étudiant qui achète des logiciels. La fédération d'identités permet cette attestation sans délivrer de liste d'étudiants aux éditeurs.

D'un point de vue plus technique, lorsqu'un utilisateur accède à une ressource avec son navigateur web (et seulement à ce moment), le fournisseur de cette ressource peut interroger le fournisseur d'identité de l'utilisateur pour obtenir des informations concernant celui-ci. Ces informations sont destinées à réaliser le contrôle de l'accès au service et/ou à le personnaliser en fonction du profil de l'utilisateur.

---

1 La fédération d'identités la plus fréquemment utilisée dans la communauté de l'enseignement supérieur est « Shibboleth ».

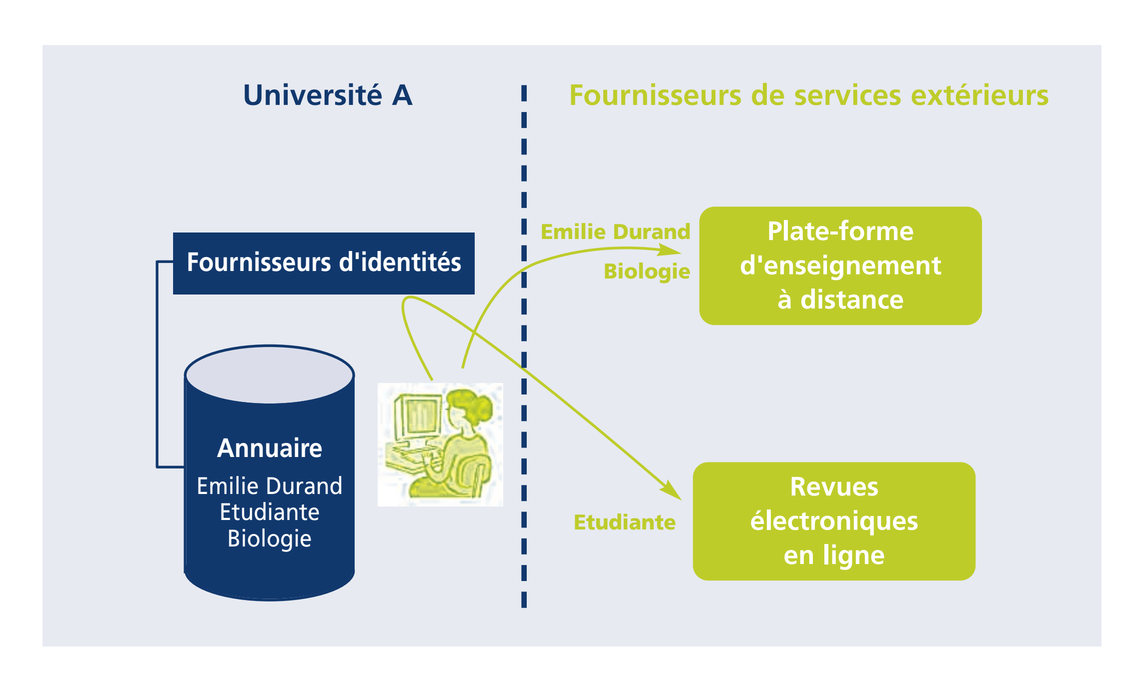
2 Cette démarche s'inscrit notamment dans le cadre de la réforme LMD (Licence-Master-Doctorat) qui permet de compléter par exemple ses modules de cours auprès d'autres établissements. La mise en place de fédération d'identités répond au besoin de partage d'applications entre institutions et de s'affranchir de la multiplication de comptes-utilisateurs.

CPU - AMUE - CNIL © 2009

Un fournisseur d'identité, à savoir l'université ou l'établissement décide par avance des informations qu'il s'autorise à diffuser aux ressources extérieures (désigné comme le « fournisseur de service »). Il diffuse telle ou telle information en fonction des besoins fonctionnels de chaque ressource, après s'être mis d'accord avec le partenaire opérant la ressource dans leur cadre contractuel classique.

La fédération d'identités est un dispositif technique permettant d'accéder sous une nouvelle forme à des informations d'un annuaire (avec une sélection stricte des informations divulguées). Pour ces accès, il est possible de consulter une entrée de l'annuaire, mais jamais de lister le contenu de l'ensemble de l'annuaire. Dans le cas où les informations divulguées n'ont pas besoin d'être nominatives, la clé de consultation n'est pas le nom d'une personne mais un identifiant qui est utilisé une seule fois.

Schéma de fonctionnement de la fédération d'identités

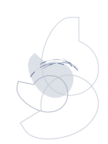


Enfin, il est à noter qu'un dispositif de fédération d'identités peut s'articuler avec les fonctionnalités d'un espace numérique de travail (ENT).

En effet, l'ENT est une offre de services purement interne à l'établissement d'enseignement avec ou sans sous-traitance pour tout ou partie des services. Le fournisseur d'identité est une extension de l'ENT qui permet l'accès à des services extérieurs à l'université opérés par des « fournisseurs de services ».

Exemples

accès à un cours en ligne opéré par une autre université et réservé à une certaine catégorie d'étudiants ; accès à des ressources documentaires proposées sur le site internet d'un éditeur privé.



En quoi mes libertés sont concernées ?

Des informations à caractère personnel (par exemple le nom, l'adresse de courrier électronique, etc.) peuvent être échangées entre les entités participant au système de fédération. Ces informations peuvent tout d'abord être excessives vis-à-vis de la finalité recherchée du service fourni ; de plus, elles doivent être échangées avec une sécurité adéquate afin de prévenir tout risque d'interception par des tiers ne faisant pas partie du système de fédération. L'enjeu est de garantir à l'utilisateur la confidentialité de ses données personnelles.

Il est essentiel que des relations de confiance existent entre les différents participants au système de fédération, que chaque traitement soit clairement identifié et soit traçable, et qu'il soit sécurisé de manière adéquate.

De plus, des informations à caractère personnel n'ont pas systématiquement besoin d'être échangées. Par exemple, pour certaines applications, les informations échangées peuvent concerner uniquement des informations génériques, par exemple le statut de la personne (étudiant, chercheur, enseignant, personnel) ou sa filière d'enseignement. Ainsi, les informations auxquelles accèdent les fournisseurs de services sont dans ces cas totalement anonymes et il convient dès lors de s'interroger au préalable sur le caractère nécessaire de l'échange de données à caractère personnel.



Que faire ?

1. Déclarer auprès de la CNIL

La fédération d'identités fait appel à deux types d'acteurs :
➢ le fournisseur d'identité qui est l'université ou l'établissement de rattachement de l'utilisateur ;
➢ les fournisseurs de services qui offrent l'accès aux ressources.

Les démarches auprès de la CNIL doivent être réalisées tant par le fournisseur d'identité qui collecte les données personnelles que par le fournisseur de service susceptible de les traiter.

- **Pour le fournisseur d'identité, à savoir l'université ou l'établissement de l'enseignement supérieur,** il appartiendra de déterminer si la diffusion de données à caractère personnel relève de la gestion administrative et pédagogique des étudiants. Dans l'affirmative, il convient de procéder à la modification de la déclaration de son fichier de gestion administrative et pédagogique des étudiants. Si l'accès à la ressource numérique n'entre pas dans ce cadre (par exemple l'accès à des services commerciaux en ligne destinés aux étudiants et qu'ils souscrivent à titre personnel), l'établissement devra procéder à une déclaration de ce traitement. Dans tous les cas de figure, l'établissement est exonéré de ces formalités dès lors qu'il a désigné un Correspondant Informatique et Libertés.

- **Pour le fournisseur de ressources, à savoir l'entité qui va mettre à disposition des ressources numériques** (ex : éditeur privé de logiciels, établissement public gérant une plate-forme d'enseignement à distance, éditeur privé de périodiques numériques), les démarches à accomplir auprès de la CNIL seront fonction de leur statut juridique :
  - ❍ s'il s'agit d'un organisme public, le traitement sera soumis à demande d'avis auprès de la CNIL (téléservice de l'administration électronique) ;

CPU - AMUE - CNIL © 2009

- si l’organisme est une personne de droit privé, le traitement sera soumis à un régime de déclaration normale.

2. Information préalable des utilisateurs

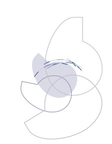
Les utilisateurs (étudiants, chercheurs et personnels) doivent être préalablement informés des informations susceptibles d’être échangées via la fédération d’identités.

Cette information préalable doit être assurée lors de la collecte des données (ex : lors de l’inscription des étudiants) ou à défaut, avant de procéder à la transmission des informations.

L'utilisateur doit également être informé de l’existence de ses droits au regard de la loi “Informatique et Libertés” au moment où il accède à la ressource numérique (ex. : mention “Informatique et Libertés” sur la page d’accueil du site web de l’éditeur).

A noter

Au cas où le destinataire des données à caractère personnel, à savoir le fournisseur de la ressource est établi en dehors de l’Union Européenne, des démarches spécifiques existent. Pour toute information complémentaire sur ces questions, consulter le dossier « International » ou le « Guide sur les transferts de données à caractère personnel vers des pays non-membre de l’Union européenne » sur le site internet de la CNIL.



Fiche n°11 Utilisation du téléphone sur le lieu de travail

De quoi s'agit-il ?

Les autocommutateurs sont des standards téléphoniques permettant d'orienter l'ensemble des appels téléphoniques entrants et sortants. Ils enregistrent ainsi les numéros d'appels composés ou reçus par les personnels ainsi que la date, heure de début, de fin et la durée de la communication.

Ils sont notamment utilisés pour :

- ➢ gérer les coûts de communication (élaboration de statistiques sur les durées moyennes d'appel et sur leur répartition géographique) ;
- ➢ permettre, le cas échéant, la facturation des appels personnels passés depuis le poste professionnel.

En quoi mes libertés sont-elles concernées ?

L'usage personnel du téléphone est possible à condition qu'une telle utilisation demeure raisonnable et ne soit pas préjudiciable à l'employeur. Il est ainsi légitime qu'un employeur s'assure du caractère non abusif de cette utilisation. Ce contrôle doit toutefois s'opérer dans des conditions propres à garantir le respect de la vie privée et des libertés des personnels sur leur lieu de travail.

En effet, un autocommutateur permet la collecte systématique de données relatives à l'identification de l'appelant.

Que faire ?

1. Encadrer l'utilisation des relevés justificatifs des numéros de téléphone appelés ou des services de téléphonie utilisés

1.1 Principe

Lorsque des relevés justificatifs des numéros de téléphone appelés sont établis, les quatre derniers chiffres de ces numéros sont occultés.

1.2 Exceptions

L'université ou l'établissement peut éditer, soit par l'intermédiaire de l'autocommutateur qu'il aura mis en place, soit par l'intermédiaire de l'opérateur auprès duquel elle ou il est client(e), l'intégralité des numéros de téléphone appelés ou le détail des services de téléphonie utilisés dans les deux cas suivants :

- ➢ dans le cas où un remboursement est demandé aux employés pour les services de téléphonie utilisés à titre privé, lorsque le montant demandé est contesté par l'employé auquel il se rapporte, un relevé justificatif complet des données relatives à l'utilisation des services de téléphonie comprenant l'intégralité des numéros de téléphone appelés peut être établi à des fins de preuves ;

CPU - AMUE - CNIL © 2009

Par ailleurs, il est recommandé de mettre en œuvre les mesures techniques permettant de sécuriser les postes (postes avec code de déverrouillage) et de pré-identifier les appels à caractère personnel ;

➢ dans le cas où l'employeur constate une utilisation manifestement anormale au regard de l'utilisation moyenne constatée des services de téléphonie au sein de l'établissement, un relevé justificatif complet des numéros de téléphone appelés ou des services de téléphonie utilisés peut être établi de façon contradictoire avec l'employé concerné.

2. Déclarer auprès de la CNIL

Si le dispositif rentre dans le cadre de la norme simplifiée n°47 adoptée par la CNIL relative à l'utilisation de services de téléphonie fixe et mobile sur les lieux de travail, il peut être déclaré en ligne sous une forme simplifiée. En cas de désignation d'un CIL, le responsable du traitement est dispensé de déclaration auprès de la CNIL.

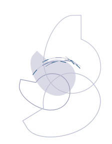
A noter

L'utilisation de téléphones mobiles est également concernée.

Attention !

Le cas particulier des salariés protégés.

En aucun cas des informations concernant leurs activités syndicales ou de représentation du personnel ne peuvent être collectées. À ce titre, une ligne déconnectée de l'autocommutateur devra être mise à leur disposition.



Fiche n°12 Mise en place des espaces numériques de travail (ENT)

De quoi s'agit-il ?

Prolongements numériques de l'université, les Espaces Numériques de Travail (ENT) sont des sites web portail permettant aux étudiants, aux enseignants, aux personnels administratifs et plus généralement à tous les membres de la communauté de l'enseignement supérieur, d'accéder, via un point d'entrée unique et sécurisé, à un bouquet de services numériques.

➢ **Un accès via internet** de son domicile ou à partir des points d'accès disponibles dans chaque établissement ;

➢ **Un accès à des contenus à vocation pédagogique et éducative**, une diffusion d'informations administratives ou relatives au fonctionnement de l'établissement, une messagerie électronique, des forums de discussion, etc.

En quoi mes libertés sont-elle concernées ?

Une attention particulière doit être portée aux mesures prises pour assurer la sécurité du dispositif.

En pratique

Elles doivent notamment garantir que chaque titulaire d'un compte ENT ne puisse accéder qu'aux seules informations le concernant. Exemple : un étudiant ne peut pas avoir accès aux notes des autres étudiants de sa promotion.
Il convient de référer aux annexes « Sécurités » du Schéma Directeur des Espaces Numériques de Travail du Ministère en particulier l'annexe « Authentification, Autorisation, SSO » qui précise les obligations à respecter en ce qui concerne la politique de gestion des mots de passe (mots de passe non stockés en clair, etc.).
Les responsables d'établissement veillent à sensibiliser les utilisateurs des ENT aux mesures élémentaires de sécurité telles que la confidentialité de leur identifiant de connexion à leur compte ENT.

Que faire ?

1. L'information des personnes est essentielle.

Chaque responsable d'établissement se doit d'informer les utilisateurs des ENT de leurs droits au regard de la loi "Informatique et Libertés".

En pratique

Cette information doit être prévue sur la page d'accueil du portail ENT et lors de la phase de création d'un compte ENT.

CPU - AMUE - CNIL © 2009

Modèle de mention d'information : « *Cet espace numérique de travail (ENT) a pour objet de proposer à la communauté universitaire des contenus à vocation pédagogique et de diffuser des informations administratives ou relatives à la vie universitaire. Chaque catégorie d'utilisateur ne peut accéder qu'aux seules informations auxquelles il a besoin d'accéder dans l'exercice de ses fonctions au sein de l'université. Conformément à la loi "Informatique et Libertés", vous disposez d'un droit d'accès, de rectification et d'opposition aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser à : [indiquez ici le service. Préciser adresse postale et adresse électronique].*

2. Les formalités auprès de la CNIL

2.1 Qui doit déclarer ?

Le président d'université ou le directeur de l'établissement d'enseignement supérieur qui a décidé de la mise en œuvre d'un ENT au sein de son établissement.

Attention !

Cette formalité subsiste quand bien même un Correspondant Informatique et Libertés a été désigné.

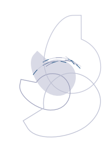
2.2 Comment déclarer ?

Les ENT sont considérés comme des téléservices de l'administration électronique. Par conséquent, le traitement relève du régime de la demande d'avis.

Une procédure de déclaration simplifiée est prévue à condition que le dispositif ENT respecte le cadre fixé par l'arrêté du 30 novembre 2006 pris après avis de la CNIL[1], à savoir notamment les finalités, les droits des personnes et les mesures de sécurité nécessaires à la protection des données à caractère personnel.

---

1 cf. Délibération n° 2006-104 adoptée par la CNIL le 27 avril 2006 portant avis sur la mise en place des espaces numériques de travail (ENT) au sein des établissements scolaires et universitaires.



Fiche n°13 Contrôle de l'utilisation des moyens informatiques

Afin d'assurer la sécurité de leur réseau et/ou de leurs ressources informatiques, les établissements peuvent être conduits à mettre en place des outils visant à contrôler l'utilisation des outils informatiques mis à disposition de leurs étudiants et de leurs personnels[1].

Ce contrôle est légitime dès lors qu'il est réalisé de manière transparente, à savoir avec une parfaite information des utilisateurs. La rédaction d'une Charte d'utilisation des outils informatiques est particulièrement utile pour rappeler les obligations mutuelles de l'établissement et de l'utilisateur, définir les modalités de contrôle qui peuvent être effectués et les sanctions auxquelles s'expose l'utilisateur s'il ne respecte pas les règles d'utilisation.

La présente fiche se propose d'aborder plus particulièrement les questions relatives à l'utilisation de la messagerie électronique et de l'internet sur le lieu de travail. Pour toute information complémentaire sur ce sujet, consulter le « Guide pratique pour les employeurs » sur le site internet de la CNIL.

A Le contrôle de l'utilisation de la messagerie électronique professionnelle

De quoi s'agit-il ?

L'utilisation de la messagerie électronique professionnelle pour envoyer ou recevoir, dans des proportions raisonnables, des messages à caractère personnel correspond à un usage généralement et socialement admis.

Il est possible de l'interdire, mais, même dans un tel cas, la nature d'une correspondance privée est protégée par « le secret des correspondances » dans le respect de la loi et de l'état actuel de la jurisprudence.

En quoi mes libertés sont-elles concernées ?

La surveillance des courriers d'un agent par sa direction doit respecter les principes issus du droit à la vie privée, même dans le cadre de la vie professionnelle. En effet, la mise en œuvre d'outils de contrôle doit s'opérer dans le respect du principe consacré à l'article 8 de la Convention européenne des droits de l'homme selon lequel : *« Le salarié a droit, même au temps et lieu de travail, au respect de l'intimité de sa vie privée ».*

---

[1] Ce contrôle est notamment réalisé à partir de la conservation de données techniques appelées données de connexion ou données relatives au trafic (ex. : adresses URL visitées, adresse IP). On sait qu'il se pose la question de savoir si les universités et les établissements de l'enseignement supérieur offrant un accès à Internet à leurs étudiants sont soumis aux dispositions de l'article L.34-1 du code des postes et des communications électroniques. Selon cet article, les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne ont l'obligation de conserver les données de connexion des personnes utilisatrices de leurs services. En tout état de cause, il convient de rappeler que cette disposition n'impose pas d'identifier les étudiants par la tenue par exemple d'un fichier des utilisateurs. Par ailleurs, afin de faciliter le travail de mise en œuvre d'une politique de gestion des traces au sein des établissements d'enseignement supérieur, le Comité de Réseaux des Universités a élaboré, sur la base de travaux du CNRS, un document « Politique type de gestion des journaux informatiques ».

CPU - AMUE - CNIL © 2009



Que faire ?

C'est la jurisprudence qui a défini les conditions dans lesquelles un employeur peut contrôler l'utilisation de la messagerie professionnelle de ses employés.

Ainsi, un arrêt de la Cour de cassation de 2001 a consacré le droit des salariés au respect de l'intimité de leur vie privée avec une interdiction pour l'employeur de prendre connaissance du contenu des correspondances qui relèveraient de la vie privée des personnes via la messagerie électronique professionnelle.

Toutefois, en 2005, la Cour de cassation[2] a reconnu à l'employeur le droit, dans certains cas, d'accéder aux fichiers personnels d'un salarié enregistrés sur le disque dur de son poste de travail. Elle pose le principe que, désormais, la nature personnelle d'un fichier ne suffit plus à le soustraire à un contrôle de l'employeur mais définit étroitement les conditions d'un tel contrôle.

Ainsi :
- ➢ par principe, l'accès à l'espace réservé à l'employé nécessite la prévision d'un tel accès dans le règlement intérieur ainsi que l'information préalable du salarié (qui doit être présent ou au moins être prévenu) ;
- ➢ par exception, le contrôle de l'espace réservé est possible sans inscription au règlement intérieur et sans information préalable en cas de « risque ou d'événement particulier ».

1. Identifier ses messages personnels

Il appartient à l'employé :
- ➢ de classer systématiquement le message dans un dossier « personnel » ;
- ➢ d'indiquer dans l'objet du message la mention « personnel » ;

2. Informer les personnes

Il est recommandé que la direction de l'établissement informe ses personnels au sujet :
- ➢ de l'existence de procédures de contrôles quant à l'utilisation de la messagerie électronique ; cette information peut être assurée par l'envoi à chaque agent d'un courrier électronique dans lequel doivent être rappelées les mentions "Informatique et Libertés". Cette information peut être utilement complétée par voie d'affichage ;
- ➢ des procédures de surveillance et d'archivage mises en œuvre pour des raisons de sécurité des systèmes d'information (ex. : encombrement du réseau);
- ➢ de la durée de conservation des données dans le cas de mesures d'archivage ;
- ➢ de l'existence et la date de la consultation préalable des instances représentatives du personnel.

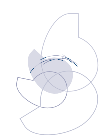
3. Rappeler les prérogatives et les obligations des administrateurs réseaux

- ➢ **Prérogatives :** accès à l'ensemble des données y compris celles qui sont sur le disque dur du poste de travail pour pouvoir travailler efficacement ; utilisation de logiciels de télémaintenance (détection de pannes ou prise de contrôle à distance[3]) ;

---

[2] COUR DE CASSATION, Chambre sociale, 17 mai 2005, Philippe X. c/ Société Cathnet-Science, N° 03-40.017 / arrêt n° 1089 – Cassation.

[3] Les logiciels de télémaintenance ou de prise de main à distance ne peuvent être utilisés par l'employeur à des fins de contrôle de l'activité de ses personnels.



➢ Obligations : l'accès aux données enregistrées par les employés (dont les correspondances personnelles) ne peut être justifié que dans le cas d'un dysfonctionnement important ; obligation de confidentialité à rappeler dans leur contrat et dans la charte d'utilisation des ressources informatiques. Respect de la durée de conservation des données indiquée dans le dossier de déclaration CNIL ou dans le registre du CIL ; en l'espèce, une durée de 6 mois à 1 an paraît raisonnable et suffisante.

Les usagers doivent être informés des prérogatives des administrateurs du réseau.

4. Déclarer à la CNIL

La mise en place d'un contrôle de la messagerie (nombre de mails entrants et sortants par employé, identification de l'émetteur et des destinataires des envois de mails, taille des fichiers transmis en pièces jointes, outil d'archivage des messages échangés…) constitue un traitement de données à caractère personnel et doit par conséquence être déclaré à la CNIL sauf en cas de désignation d'un CIL.

A noter

Accès aux données informatiques en cas d'absence d'un employé
L'obligation de loyauté impose à l'employé absent de son poste de travail de communiquer à l'employeur qui en fait la demande tout document nécessaire à la poursuite de l'activité de l'établissement. Pour autant, les modalités d'accès de l'employeur aux données stockées sur l'environnement informatique d'un employé absent (messagerie, fichiers, supports de stockage) devraient être préalablement définies en concertation et diffusées auprès de l'ensemble des employés susceptibles d'être concernés (via une charte par exemple).

B Le contrôle de l'utilisation de l'internet

De quoi s'agit-il ?

Une interdiction générale et absolue de toute utilisation d'internet à des fins autres que professionnelles ne paraît pas réaliste dans une société de l'information et de la communication, et semble de plus disproportionnée au regard des textes applicables et de leur interprétation par la jurisprudence.

Un usage raisonnable du personnel, non susceptible d'amoindrir les conditions d'accès professionnel au réseau ne mettant pas en cause la productivité est généralement et socialement admis par la plupart des entreprises ou administrations.

Que faire ?

1. Rédiger une « charte » d'utilisation d'internet au sein de l'établissement

Celle-ci peut notamment prévoir :

➢ la mise en place de dispositifs de filtrage de sites non autorisés, associés au pare-feu (sites diffusant des produits à caractère pornographiques, pédophiles, incitation à la haine raciale, révisionnistes, etc.) comme une mesure de prévention ;

CPU - AMUE - CNIL © 2009

- aux fins de sécurité, l'interdiction de télécharger des logiciels, de se connecter à un forum ou d'utiliser le « chat », d'accéder à une boîte aux lettres personnelle par internet compte tenu des risques de virus.

2. Informer les personnes

Les modalités d'un tel contrôle de l'usage d'internet doivent faire l'objet d'une consultation des instances représentatives du personnel et d'une information des utilisateurs, y compris lorsque le contrôle est dépourvu d'un caractère directement nominatif.

3. Déclarer auprès de la CNIL

Un contrôle a posteriori des données de connexion à internet, restitué de façon globale, par exemple au niveau de l'organisme ou d'un service déterminé, devrait dans la plupart des cas être suffisant sans qu'il soit nécessaire de procéder à un contrôle individualisé des sites visités par un employé déterminé.

Toutefois, si l'établissement met en place un dispositif de contrôle individuel des employés destiné à produire, poste par poste, un relevé des durées de connexion ou des sites visités, le traitement automatisé de données à caractère personnel ainsi mis en œuvre doit être déclaré à la CNIL (sauf désignation d'un Correspondant Informatique et Libertés).

La durée pendant laquelle les relevés ainsi établis sont conservés doit être précisée. Une durée de conservation de l'ordre de six mois devrait être suffisante, dans la plupart des cas, pour dissuader tout usage abusif d'internet. Le dossier de déclaration doit en outre comporter l'indication et la date à laquelle les instances représentatives du personnel ont été consultées sur de tels dispositifs.

En pratique

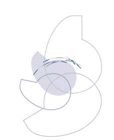
L'utilisation par les organisations syndicales de l'intranet et de la messagerie électronique de l'université ou l'établissement d'enseignement

Les universités ou les établissements devraient négocier les conditions dans lesquelles leur messagerie et/ou leur intranet peuvent être utilisés par les instances représentatives du personnel ou pour l'exercice d'un mandat syndical. À titre indicatif, la Cour de cassation a considéré en juin 2007[4] qu'en l'absence d'accord et dans la mesure où l'employeur a déjà toléré une utilisation de l'intranet à des fins syndicales par le passé, une telle utilisation ne constituerait pas une faute pour le salarié.

A priori, les adresses de messagerie électronique des employés peuvent être utilisées par les organisations syndicales pour la mise à disposition de publications et tracts de nature syndicale à condition que les employés en soient informés pour pouvoir s'opposer au préalable à l'envoi de tout message à des fins de prospection syndicale sur leur messagerie professionnelle. Lorsque les instances représentatives du personnel disposent d'un compte de messagerie dédié, des mesures de sécurité particulières devraient être mises en œuvre afin d'assurer la confidentialité des informations échangées.

---

[4] Cour de cassation Chambre sociale Arrêt du 27 juin 2007, Oce Business services / Michel B.



Fiche n°14 Création de sites internet (site web, blog, ...)

De quoi s'agit-il ?

Des sites web peuvent être créés dans le cadre d'activités professionnelles (ex. : site web de l'université, site d'un enseignant-chercheur présentant ses travaux), syndicales, politiques ou associatives.

Les sites personnels, par ailleurs plus connus sous le nom de « blog », ont pour vocation la diffusion d'informations à destination du cercle familial ou des proches, la mise en ligne d'un journal personnel (blocs-notes ou « blog ») ou la présentation de sujets d'intérêt personnel (loisirs, sport, culture, diffusion d'idées, etc.).

En quoi mes libertés sont-elles concernées ?

Du fait de sa mise en ligne sur le réseau internet, un site web constitue un espace ouvert au public. Aussi, la diffusion de données à caractère personnel sur ces sites est-elle susceptible de porter atteinte à la vie privée des personnes dès lors qu'elles n'ont pas été préalablement informées d'une telle diffusion.
De plus, l'existence de moteurs de recherche de plus en plus performants multiplie les risques en matière d'atteinte à la vie privée. En effet, l'utilisation des moteurs de recherche à partir du nom d'une personne permet d'accéder à l'ensemble des pages web où est diffusé ce nom (possibilité de reconstituer une « biographie » virtuelle des personnes - utilisation par des employeurs par exemple dans le cadre d'une embauche).



Exemple

La CNIL a ainsi veillé à ce que certaines sanctions disciplinaires du ministère de l'Éducation nationale ne soient accessibles qu'aux seules personnes qui y sont habilitées, et non plus diffusées à partir des sites web des ministères concernés auxquels chacun peut avoir accès.

Que faire ?

La mise en ligne d'un site web, que celle-ci soit effectuée dans un cadre privé ou professionnel, doit s'effectuer dans le respect d'un certain nombre de règles. Un site web ne doit pas être considéré comme une « zone de non-droit ».
Ainsi par exemple, la diffusion de propos diffamatoires, d'injures ou propos racistes sur un site peut être pénalement sanctionnée. Des sanctions disciplinaires pourraient également être prononcées à l'encontre d'un étudiant qui aurait tenu sur son « blog » des propos calomnieux ou injurieux à l'égard du corps enseignant et administratif de son établissement.
Enfin, dès lors qu'un site web diffuse ou collecte des données à caractère personnel, celui-ci est soumis au respect des dispositions de la loi "Informatique et Libertés".

CPU - AMUE - CNIL © 2009

En pratique

Les sites web personnels (« blog »)

➢ Ces sites n'ont pas à être déclarés auprès de la CNIL (dispense adoptée par la CNIL en 2005) ;

Attention !

La diffusion et la collecte de données à caractère personnel opérées à partir d'un site web dans le cadre d'activités professionnelles, politiques, ou associatives restent soumises à l'accomplissement des formalités préalables prévues par la loi.

➢ il est recommandé[1] lors de la mise en œuvre de « blog » :

- de prévoir un accès restreint au bénéfice des seules personnes identifiées par le responsable du site. Lorsqu'un particulier souhaite créer un site au bénéfice de ses proches aux fins de diffusion, par exemple, de photographies d'un événement (mariage, anniversaire, etc.), il est important au regard de la nature du réseau internet que soient mis en place des dispositifs permettant de limiter cette diffusion aux seules personnes concernées ;
- de recueillir le consentement préalable des personnes dont les données sont diffusées sur le site ;
- de ne pas diffuser des données dites sensibles (ex. opinion politique) qui n'ont pas vocation à être diffusées à partir d'un site internet ouvert au public ;
- de prévoir pour toute personne dont les données à caractère personnel sont diffusées à partir d'un site web la faculté de s'opposer à tout moment à cette diffusion.

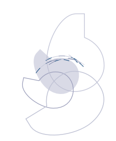
En ce qui concerne les sites web qui ne seraient pas créés dans le cadre d'une activité exclusivement personnelle tel que par exemple le site institutionnel de l'université, ils sont également soumis aux dispositions de la loi "Informatique et Libertés".

Ainsi, par exemple :

➢ lors de la collecte de données à caractère personnel (ex. : abonnement à la lettre d'information), les personnes auprès desquelles sont recueillies les informations doivent être informées de la finalité de cette collecte, des destinataires ou catégories de destinataires des données et de l'existence d'un droit d'accès, de rectification et d'opposition (se reporter à l'annexe 1 pour un modèle de mention d'information) ;

➢ la diffusion de la photographie des étudiants et des personnels sur ce site est subordonnée au recueil du consentement des personnes concernées.

[1] Cf. délibération n° 2005-285 adoptée par la CNIL le 22 novembre 2005 portant recommandation sur la mise en œuvre par des particuliers de sites web diffusant ou collectant des données à caractère personnel dans le cadre d'une activité exclusivement personnelle.



Fiche n°15 Enregistrement et utilisation du numéro de sécurité sociale



De quoi s'agit-il ?

Le NIR, numéro d'inscription au Répertoire National d'Identification des Personnes Physiques (RNIPP), communément appelé numéro de sécurité sociale, est un élément d'identification des personnes physiques. La gestion du NIR est confiée à l'INSEE.

En quoi mes libertés sont concernées ?

Le NIR n'est pas un numéro comme les autres.

Il est particulier car il est :
- signifiant – il est composé d'une chaîne de caractères qui permettent de déterminer le sexe, le mois et l'année de naissance, et dans la majorité des cas, le département et la commune de naissance en France ou l'indication d'une naissance à l'étranger ;
- unique et pérenne – un seul numéro est attribué à chaque individu dès sa naissance.

La loi "Informatique et Libertés" a toujours soumis à des exigences procédurales particulières l'utilisation du NIR ou, ce qui a été considéré comme revenant au même, le recours au RNIPP. En effet, les craintes suscitées par la généralisation d'un identifiant national et unique qui rendrait plus aisées les possibilités de rapprochements de fichiers ont conduit le législateur à encadrer strictement l'utilisation de ce numéro.

Que faire ?

Lorsqu'un établissement envisage l'enregistrement et/ou l'utilisation du NIR, il doit tout d'abord s'assurer du fait que cette utilisation est légale.

En effet, l'enregistrement du numéro de sécurité sociale dans un traitement est notamment autorisé :
- dans les fichiers de paie et de gestion du personnel pour l'établissement des bulletins de paie et des différentes déclarations sociales obligatoires (décret n° 91-1404 du 27 décembre 1991) ;
- dans le cadre de la prise en charge des frais de maladie (articles R.115-1 et R.115-2 du code de la sécurité sociale).

Exemple

L'immatriculation des étudiants à la sécurité sociale lors de l'inscription dans l'établissement.

CPU - AMUE - CNIL © 2009

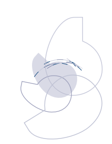
Les états produits et les documents édités ne peuvent donc porter mention de ce numéro que dans le cadre des opérations précitées.

Cette règle s'applique même dans le cas de logiciels intégrés de gestion et de paie qui doivent être paramétrés pour limiter l'utilisation du numéro de sécurité sociale aux seules opérations précédemment décrites.

En particulier, le numéro de sécurité sociale ne fait pas partie de la liste des informations qui doivent figurer dans le registre unique du personnel, fixée par les articles L.620-3 et R. 620-3 du code du travail, et ne doit donc pas être enregistré dans ce cadre.

Le numéro de sécurité sociale d'un employé ne peut donc pas être utilisé comme numéro de matricule unique pour l'identifier dans tous les fichiers de gestion des ressources humaines de son entreprise ou de son administration.

En dehors des cas visés ci-dessus, l'utilisation du numéro de sécurité sociale ne peut être autorisée que dans le cadre d'un décret en Conseil d'État ou arrêté pris après avis de la CNIL.



Fiche n°16 Communication à des tiers autorisés d'informations relatives aux personnels et aux étudiants

De quoi s'agit-il ?

la loi permet à des autorités publiques de se faire communiquer, dans le cadre de leurs missions et sous certaines conditions, des informations issues de fichiers. il sagit du cas des « tiers autorisés ».

En quoi mes libertés sont-elles concernées ?

Certaines administrations sont autorisées par la loi à se faire communiquer ponctuellement des informations afin d'assurer leurs missions d'intérêt général.

Afin de protéger les libertés, il reviendra aux responsables de cette communication de s'assurer que le demandeur correspond bien à l'un de ceux qui sont autorisés.

Le fait, pour un responsable du traitement, de porter à la connaissance d'un tiers qui n'a pas qualité pour les recevoir des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée constitue une infraction pénale punie de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Que faire ?

1. Dans quelles conditions un établissement peut-il communiquer à des « tiers autorisés » des renseignements sur ses personnels et ses étudiants ?

Cette communication ne peut être effectuée que **sur demande ponctuelle écrite**, visant des personnes nommément désignées, identifiées directement ou indirectement. Il est exclu qu'elle porte sur l'intégralité d'un fichier. L'établissement n'est pas tenu de répondre à une simple demande téléphonique qui ne lui permettra pas de s'assurer de la qualité de son interlocuteur.

La demande doit préciser le **texte législatif fondant ce droit de communication**, ainsi que les catégories d'informations sollicitées. L'établissement saisi de la requête doit s'assurer de sa conformité aux textes invoqués et peut toujours, en cas de doute, interroger la CNIL.

2. Quels sont les tiers autorisés à obtenir ponctuellement des informations personnelles détenues par les établissements ?

2.1 L'administration fiscale

➢ Le Trésor public (direction générale de la comptabilité publique uniquement dans les conditions fixées par les articles L.81 à L.95 du Livre des Procédures fiscales pour le recouvrement de créances fiscales ou des amendes et condamnations pécuniaires).

➢ La direction générale des impôts ou la direction générale des douanes en vue de l'établissement de l'assiette, du contrôle, du recouvrement des impôts (articles L. 81 à L. 95 du Livre des procédures fiscales).

CPU - AMUE - CNIL © 2009

2.2 Les organismes sociaux

- Les organismes débiteurs de prestations familiales ou en charge du versement du RMI dans les conditions prévues par l'article L.583-3 du code de la sécurité sociale.
- Les organismes débiteurs de prestations familiales ou les huissiers de justice au titre de leur mission de recouvrement des créances alimentaires impayées (article 7 de la loi 73-5 du 2 janvier 1973).

2.3 Les administrations de la justice, de la police et de la gendarmerie

- Les magistrats, dans le cadre des dispositions des codes de procédure pénale et de procédure civile (notamment les articles 56, 57, 92 à 97 du code de procédure pénale).
- Le procureur de la République, à la demande de l'huissier de justice porteur d'un titre exécutoire et au vu d'un relevé certifié sincère des recherches infructueuses qu'il a tentées pour l'exécution (article 40 de la loi n° 91-650 du 9 juillet 1991).
- Les officiers de police judiciaire de la police et de la gendarmerie nationales agissant en flagrant délit, sur commission rogatoire ou dans le cadre d'une enquête préliminaire (articles 57-1, 60-1 et 76-3 du code de procédure pénale) y compris par voie informatique ou télématique (article 60-2 du même code).
- Les bureaux d'aide judiciaire afin de demander la vérification des ressources en vue de l'attribution de l'aide judiciaire (loi n° 72-11 du 3 janvier 1972 modifiée par la loi du 31 décembre 1982 relative à l'aide judiciaire).

2.4 Les autres administrations bénéficiant d'un droit de communication

- Les services déconcentrés du travail et de l'emploi dans le cadre du contrôle de la recherche d'emploi (ordonnance n°86-1286 du 20 décembre 1986, articles L. 351-1 et R. 351-32 du code du travail).
- Les services en charge de la gestion des allocations supplémentaires prévues aux articles L 815-2 et 3 du code de la sécurité sociale (fonds de solidarité vieillesse et fonds spécial d'invalidité) pour le recouvrement sur la succession des héritiers (articles L. 815-12 et L. 815-15 du code de la sécurité sociale).

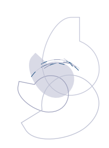
Aucun fondement législatif n'autorise par principe la communication d'informations aux particuliers ou à des sociétés privées.

De façon générale, l'établissement ne peut, sauf cas des tiers autorisés prévus par la loi, communiquer à des tiers des informations nominatives relatives à ses personnels et/ou ses étudiants que dans la mesure où ces derniers en ont été préalablement informés et ne s'y sont pas opposés.

En outre, il s'assurera de la mise à jour de sa déclaration auprès de la CNIL car il s'agira, *a priori*, d'un destinataire qui n'a pas été indiqué initialement dans le dossier de déclaration.

Une notification doit donc être adressée :

- soit au Correspondant à la protection des données de l'établissement afin qu'il procède à la mise à jour de son registre des traitements ;
- soit à la CNIL.



Exemples

Communication du fichier de gestion du personnel à des mutuelles de l'éducation nationale.

L'établissement doit veiller à ce que cette transmission réponde à une finalité qui soit légitime et explicite. Cette transmission ne devrait servir qu'à permettre une mise à jour de la base de données de la mutuelle et en aucun cas, à assurer la promotion de la mutuelle complémentaire. En outre, les personnes concernées devront être préalablement informées de cette transmission et être mises en mesure de s'y opposer.

CPU - AMUE - CNIL © 2009

Fiche n°17 Utilisation de la biométrie



De quoi s'agit-il ?

Cette technique consiste à appliquer des traitements informatiques aux caractéristiques physiques (contours ou forme de la main ou du visage, dessins de l'iris, empreinte digitale ou palmaire, etc.) des personnes[1].

Elle est principalement utilisée pour renforcer la sécurité des accès à des locaux.



En quoi mes libertés sont-elles concernées ?

Du fait des dangers potentiels liés à l'exploitation de ces caractéristiques physiques, qui sont propres à chaque être humain et dont certaines (empreintes digitales, ADN…) peuvent être collectées à l'insu des intéressés, les traitements faisant appel à un dispositif biométrique **sont soumis par la loi à un régime d'autorisation préalable de la CNIL.**



Que faire ?

D'une manière générale, il existe deux types de procédures pour notifier à la CNIL l'utilisation d'applications biométriques. La détermination de la procédure applicable est essentiellement fonction de la biométrie choisie, ainsi que du contexte d'utilisation.

1. La procédure d'autorisation au cas par cas pour les dispositifs biométriques

➢ reposant sur un enregistrement de l'empreinte digitale dans une base de données centralisée ou dans le lecteur.
Ils doivent être justifiés par l'existence d'un fort impératif de sécurité.

Exemple

Le contrôle de l'accès aux locaux sensibles où sont conservés les sujets nationaux d'examens et de concours.

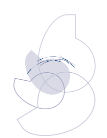
➢ Reposant sur des caractéristiques biométriques telles que le visage, l'iris ou la voix.

En pratique

Comment déclarer ?
Les établissements, y compris ceux ayant désigné un Correspondant Informatique et Libertés, doivent adresser à la CNIL une demande d'autorisation constituée d'un formulaire de déclaration normale dûment rempli, accompagné :
- des annexes « Sécurités » disponibles sur le site de la CNIL ;
- tout élément justifiant la mise en place d'un dispositif biométrique ;
- toute documentation technique relative au dispositif utilisé.

---

[1] Elle repose plus précisément sur le traitement du « gabarit » de la caractéristique physique concernée. Ce gabarit constitue un identifiant unique, calculé sur la base des points propres à la caractéristique physique utilisée. Ce n'est donc pas une image, photographie de la donnée, qui est traitée mais sa retranscription au format numérique grâce à un algorithme (formule mathématique).



2. La procédure d'engagement de conformité à une autorisation unique adoptée par la CNIL pour les dispositifs biométriques reposant sur :

- ➢ le contour de la main pour contrôler l'accès et la gestion des horaires et de la restauration sur les lieux de travail ;
- ➢ l'empreinte digitale exclusivement enregistrée sur un support individuel (carte à puce, clé USB) détenu par la personne concernée pour contrôler l'accès aux locaux professionnels[2].

En pratique

Comment déclarer ?
Si le traitement est strictement conforme à l'une de ces autorisations uniques, une simple déclaration de conformité suffit[3]. Elle peut être effectuée en ligne, à partir du site web de la CNIL. Cette formalité est requise y compris si l'établissement a désigné un Correspondant Informatique et Libertés.

Attention !

La norme simplifiée n° 42, relative à la gestion des contrôles d'accès aux locaux, des horaires et de la restauration n'est pas applicable aux applications faisant appel à un procédé de reconnaissance biométrique.

[2] Cette autorisation unique ne s'applique pas aux dispositifs qui reposent sur l'enregistrement de la donnée biométrique dans une base de données qu'elle soit stockée sur le terminal de lecture comparaison ou sur un serveur.
[3] Voir le tableau synthétique figurant en annexe n°1.

CPU - AMUE - CNIL © 2009

Fiche n°18 Dispositifs de vidéosurveillance

De quoi s'agit-il ?

La vidéosurveillance consiste à placer des caméras de surveillance dans un lieu public ou privé, pour prévenir des actes de malveillance. Elles peuvent être fixes ou mobiles, automatiques ou télécommandées.



En quoi mes libertés sont-elles concernées ?

Les systèmes de vidéosurveillance peuvent intrinsèquement porter atteinte aux libertés individuelles (par exemple, à la liberté d'aller et venir). Il est dès lors nécessaire d'accompagner leur mise en œuvre d'un certain nombre de garanties.



Que faire ?

1. Une réflexion préalable indispensable

Une réflexion préalable à la décision d'utiliser un système de vidéosurveillance, comportant notamment une analyse précise des risques tenant compte des incidents survenus dans l'enceinte de l'établissement devrait être menée de façon à identifier les solutions alternatives permettant d'atteindre l'objectif poursuivi sans recourir à ce moyen (une sécurisation des accès aux moyens de badges magnétiques, surveillance renforcée par les personnels, une modification des heures d'ouvertures de certaines issues peuvent par exemple constituer des réponses efficaces et adaptées à un objectif particulier de sécurisation).

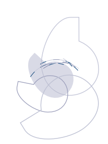
2. Le nécessaire respect du principe de proportionnalité

Si le déploiement de tels dispositifs répond généralement à un objectif sécuritaire (contrôle des accès aux locaux), il ne peut avoir pour objectif la mise sous surveillance spécifique d'un employé déterminé ou d'un groupe particulier de personnes. Le nombre, l'emplacement, l'orientation, les fonctionnalités et les périodes de fonctionnement des caméras, ou la nature des tâches accomplies par les personnes devant être soumises à la vidéosurveillance, sont autant d'éléments devant notamment entrer en ligne de compte lors de l'évaluation du caractère proportionné du système.

Exemples

Certains systèmes de vidéosurveillance sont susceptibles de présenter un caractère illégal :

- un système qui serait installé dans un lieu susceptible de porter atteinte à l'intimité de la vie privée des personnes (vestiaires, douches, toilettes) ;
- un système qui serait installé de façon à enregistrer de façon spécifique les allées et venues des personnes se rendant dans un local syndical.



3. L’obligation d’information

Il ne doit pas y avoir de surveillance à l’insu des personnes concernées à savoir des enseignants, des étudiants, des personnels et des visiteurs.

L’existence de système de vidéosurveillance doit être portée à la connaissance de toute personne filmée ou susceptible de l’être de façon claire et permanente par exemple au moyen de panonceaux apposés à l’entrée des locaux (exemple fourni ci-dessous).

Les instances représentatives du personnel doivent être consultées avant toute mise en œuvre d'un système de vidéosurveillance et précisément informées des fonctionnalités envisagées.

4. L’élaboration d’un document de référence

Il est recommandé d’établir un document identifiant clairement les objectifs et les modalités d’utilisation du système de vidéosurveillance, les personnes habilitées et formées à visionner les images, la durée maximale de conservation et les modalités d’exercice du droit d’accès aux images.

5. Une visualisation des images restreinte aux seuls destinataires habilités

Les images enregistrées ne peuvent être visionnées que par les seules personnes dûment habilitées à cet effet, dans le cadre de leurs attributions respectives (par exemple : le responsable de la sécurité de l’organisme). Ces personnes devraient être particulièrement formées et avoir été sensibilisées aux règles encadrant la mise en œuvre d’un système de vidéosurveillance.

6. Une durée de conservation des images limitée

Sauf enquête ou information judiciaire, la durée de conservation des images enregistrées à l’aide d’un dispositif de vidéosurveillance ne devrait pas excéder quelques jours et les enregistrements doivent être détruits par la suite. Cette durée ne peut en tout état de cause s’étendre au delà d’un mois.

7. La nécessité d’accomplir certaines formalités préalables

Un système de vidéosurveillance numérique mis en place dans les enceintes et locaux affectés à titre principal à l’établissement ne peut être installé que s’il a préalablement fait l’objet d’une déclaration auprès de la CNIL. Celle-ci précisera notamment les justifications particulières qui ont conduit à l’installation d’un dispositif de vidéosurveillance. Le traitement est toutefois dispensé de déclaration en cas de désignation d’un Correspondant Informatique et Libertés.

CPU - AMUE - CNIL © 2009

Attention !

L'installation d'un système de vidéosurveillance sur la voie publique ou dans un lieu ouvert au public[1] est subordonnée à l'obtention d'une **autorisation préfectorale**.

Exemple

Le système est implanté sur la voie publique pour filmer les abords de l'université ou les parties du domaine universitaire qui sont ouvertes au public.

Attention !

Si le système prévu devait s'accompagner d'un dispositif de reconnaissance faciale, il devrait alors faire l'objet d'une demande d'autorisation à la CNIL dans la mesure où il fait appel à une technique biométrique[2].

Exemple d'information à diffuser

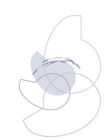
Établissement sous vidéosurveillance

Nous vous informons que cet établissement est placé sous vidéosurveillance pour des raisons de … [indiquer les finalités poursuivies]. Pour tout renseignement, s'adresser au service … ou à … [identifier la personne ou le service compétent], auprès duquel vous pouvez également exercer votre droit d'accès, conformément à la loi “Informatique et Libertés”.

---

1 Pour savoir si le dispositif est considéré comme installé sur la voie publique et donc soumis à autorisation préfectorale, l'arrêté pris, le cas échéant, par le recteur chancelier des universités qui délimite les enceintes et locaux affectés à titre principal à un établissement peut être pris en considération. Par ailleurs, pour savoir s'il est installé dans un lieu ouvert au public, il appartiendra à chaque établissement de le déterminer en fonction des délimitations physiques ou matérielles (clôtures, contrôles d'accès,…). Sur ce point précis, la circulaire du 22 octobre 1996 relative à l'application de l'article 10 de la loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité indique que, selon la jurisprudence, un lieu public est « un lieu accessible à tous, sans autorisation spéciale de quiconque, que l'accès en soit permanent et inconditionnel ou subordonné à certaines conditions ». (par exemple acquittement d'un droit d'entrée). Voir à ce propos le jugement du tribunal de grande instance de Paris du 23 octobre 1986, Gazette du Palais du 8 janvier 1987, confirmé par l'arrêt de la cour d'appel de Paris du 19 novembre 1986. »

2 Se reporter à la fiche 17 sur la biométrie.



Fiche n°19 Mise en place d'une carte étudiante multiservices

De quoi s'agit-il ?

La carte multiservices est un outil « multi-partenaires » de l'Université et du CROUS.

La carte a trois grandes fonctions :

- identifier l'étudiant par les inscriptions visibles sur la carte (nom, prénom, photo, code d'identifiant national étudiant (INE), identifiant numérique (accès réseau) et code APOGEE (local, chiffre et code barre) ainsi que par des informations plus complètes embarquées dans une puce (reprises du logiciel APOGEE). Cette identification permet d'offrir une éventuelle base à des évolutions pour des usages internes (accès sportif, vote étudiant,…) et externes (accès aux musées, transports,…) ;
- permettre un contrôle d'accès grâce à la puce qui contient les informations précédentes qui ouvrirait droit à des contrôles d'accès divers (bibliothèque,…) ;
- servir de porte-monnaie électronique en assurant les paiements avec authentification du droit et du tarif d'accès aux Restaurants Universitaires.

Les deux premières applications sont gérées par l'Université et la troisième est une demande du CROUS dans le cadre d'une démarche nationale.

Les données visuelles sont très limitées, mais suffisantes à une reconnaissance du porteur. Les données numériques embarquées ne sont lisibles qu'à partir de lecteurs spécifiques (services de la scolarité et restaurants universitaires) dont l'utilisation nécessite des autorisations précises (identifiant et mot de passe) délivrés par les responsables de la mise en place de la carte.

En quoi mes libertés sont-elles concernées ?

Une carte étudiant multiservices contient de nombreuses informations destinées à des entités externes à l'établissement et est susceptible d'exiger des interconnexions entre systèmes. Dans ce contexte, il est important de limiter la diffusion des informations aux seules entités qui en ont besoin dans leur relation avec les étudiants.

Que faire ?

Au préalable, il existe un certain nombre de questions techniques à se poser afin notamment d'identifier les formalités à accomplir.

- Quelle est l'architecture technique du projet et plus particulièrement quelles sont les flux d'informations entre les différents intervenants lors de la création du compte et de son utilisation par les différents services ?
- Le dispositif suppose-t-il l'interconnexion de fichiers existants avec le dispositif de gestion de la Carte Multiservices ou fonctionne-t-il de façon indépendante des « applications métiers » des partenaires concernés ?
- Quelles sont les informations mutualisées ? Et entre quels intervenants le sont-elles (tous ou seulement ceux concernés par les activités choisies par une personne déterminée) ? ;

CPU - AMUE - CNIL © 2009

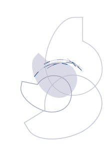
- Comment se fait l'identification des titulaires de carte ? Cette identification est-elle commune à l'ensemble du dispositif ou y a-t-il autant d'identifiants qu'il y a de cartes associées à un compte donné ? Quelles sont les modalités d'identification des usagers ?

- Est-ce que le dispositif repose sur la mise en place d'un téléservice de l'administration électronique (ex : l'étudiant pourra accéder au compte de sa carte via Internet à partir d'identifiants de connexion qui lui sont propres). Dans ce cas de figure, le traitement est soumis au régime de la demande d'avis (cf. article 27, II, 4° de la loi).

Par ailleurs, il faudra veiller au respect des principes fondamentaux de la protection des données personnelles (finalités, proportionnalité, information des personnes, droit à l'oubli, etc.).

Attention !

Les cartes devront offrir un niveau de sécurité approprié compte tenu de l'état de la technologie, de la nature sensible ou non des données enregistrées, du nombre et du type d`applications prévues et de l'évaluation des risques potentiels. Les modalités selon lesquelles les tiers peuvent avoir accès aux données enregistrées sur la carte doivent être établies au préalable pour chacune des finalités spécifiques pour lesquels la carte est utilisée.
Lors de l'émission d'une carte, le porteur devrait être dûment informé de la manière d'utiliser sa carte ainsi que des mesures à prendre en cas de fraude ou de divulgation non autorisée.



Fiche n°20 Tenue de listes de contacts pour un colloque scientifique organisé par une Unité Mixte de Recherche



De quoi s'agit-il ?

Une Unité Mixte de Recherche (UMR) souhaite organiser un colloque scientifique. Pour ce faire, une procédure d'inscription – en ligne et/ou hors ligne - est prévue afin d'organiser cette manifestation. Un fichier comportant des informations personnelles sur les participants à ce colloque est ainsi créé au sein de l'UMR.



En quoi mes libertés sont-elles concernées ?

Ce cas aborde la question de la détermination du responsable du traitement dans le cadre de la mixité de certaines unités des universités. La difficulté à identifier précisément ce responsable fait courir un risque de non-respect des formalités par l'un et l'autre des établissements, ce qui nuirait tant aux établissements qu'au respect des droits des participants (déclaration, exercice du droits d'accès, de rectification et d'opposition notamment en cas de cession des données à des partenaires du colloque…).

Que faire ?

Le responsable du traitement est le directeur de l'UMR, organisatrice du colloque.

Cependant, le Directeur en question peut relever, administrativement, de l'organisme de recherche ou de l'université (personnel chercheur ou enseignant-chercheur). Ainsi, se pose la question de la personne morale qui devra procéder à la déclaration.

À ce sujet, l'organisme déclarant peut être indifféremment l'université ou l'organisme puisque les deux assument la tutelle de l'unité. Il leur reviendra donc, afin d'assurer la plus grande sécurité juridique, de définir dans les conventions qui les lient celui d'entre eux qui aura cette responsabilité, unité par unité (cf fiche n°1 sur la notion de responsable du traitement).

Par ailleurs, les données ne peuvent être transmises aux partenaires du colloque que si une mention a été expressément portée à la connaissance des participants au moment de leur inscription et leur accord recueilli.

Dans l'hypothèse où l'UMR envisage d'utiliser sa base de données en vue d'un nouveau colloque, elle ne pourra le faire qu'à la condition que les personnes aient été mises en mesure de s'y opposer lors de la collecte initiale de ces données (1ère inscription).

Dans le cas d'une inscription payante en ligne, l'UMR devra s'assurer que la transaction est sécurisée (exemple : utilisation du protocole SSL).

Enfin, rappelons que la durée de conservation ne peut excéder celle strictement nécessaire aux finalités du traitement.

En pratique

Les données devraient être supprimées à l'issue de l'envoi des actes du colloque sauf si les participants ont accepté d'être informés par la suite de la tenue de nouveaux colloques.

CPU - AMUE - CNIL © 2009

Fiche n°21 Les consultations par voie électronique



De quoi s'agit-il ?

Dans certaines occasions, les établissements peuvent avoir besoin de consulter les étudiants par voie électronique.

Exemple

- Lors de mouvements universitaires, certains établissements souhaitent organiser la consultation des étudiants par voie électronique sur des questions relatives au blocage des locaux et à la reprise des cours.
- Un établissement peut vouloir solliciter l'avis des étudiants sur une question liée à la vie étudiante.

Cette consultation ne peut être qualifiée d'élection dans la mesure où elle ne conduit pas à la désignation d'une personne pour occuper une fonction au sein de l'établissement. Elle est néanmoins soumise au respect de la loi « Informatique et Libertés », notamment en matière de mesures prises pour assurer la sécurité et la confidentialité des données. En effet, ces mesures s'imposent afin de garantir la validité de la consultation.



En quoi mes libertés sont-elles concernées ?

Les consultations par voie électronique nécessitent l'utilisation de données à caractère personnel. Il est essentiel de garantir le secret de l'opinion émise, ainsi que la sécurité et l'intégrité des échanges.

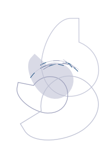


Que faire ?

Afin de garantir la légitimité des résultats, l'organisation d'une consultation par voie électronique doit respecter les mêmes principes de sécurité qu'une élection par voie électronique (cf. fiche n°22). Les personnes consultées doivent également être clairement informées de la finalité et des modalités d'organisation de la consultation envisagée.

Cette consultation peut s'appuyer sur les dispositifs d'authentification de l'ENT (Espace Numérique de Travail). Dans ce cas, il est nécessaire que les mécanismes mis en jeu séparent les données d'authentification du compte ENT du fichier des réponses, afin de garantir l'anonymat des votes. La procédure doit être déclenchée et close par un dispositif permettant une traçabilité (impression de pages en présence d'un huissier, de représentant du conseil d'administration,…).

Dès lors que la consultation en ligne concerne les étudiants, il s'agit d'un téléservice de l'administration électronique, soumise à avis de la CNIL. Les formalités sont donc identiques dans ce cas à celles du vote électronique pour les étudiants.



Exemple

Le projet de décision peut porter sur la consultation de tous les étudiants régulièrement inscrits à l'Université, à l'initiative du Président de l'Université, sur toute question relative à l'organisation des études et à la vie étudiante.
Ce type de formulation permet de prendre en compte différents sujets sur lesquels les étudiants pourraient être consultés.

Toutefois, un nouveau dossier de demande d'avis doit être déposé à la CNIL en cas de changement du dispositif technique.

CPU - AMUE - CNIL © 2009

Fiche n°22 Elections par voie électronique



De quoi s'agit-il ?

Les établissements d'enseignement supérieur et les organismes de recherche peuvent être amenés à organiser des opérations de vote électronique pour élire leurs représentants.

Exemple

- l'élection des représentants des étudiants aux conseils centraux des universités.
- l'élection des représentants au conseil d'administration du CNRS.

Il s'agit d'opérations électorales, qui peuvent être organisées dans des bureaux de vote au sein desquels est installé un dispositif de vote électronique (cas des élections dans les conseils centraux des universités), ou bien via internet, depuis tout poste professionnel ou personnel, afin de permettre au plus grand nombre de votants de participer (cas du CNRS).



En quoi mes libertés sont-elles concernées ?

Les élections par voie électronique nécessitent l'utilisation de données à caractère personnel. Il est essentiel de garantir le secret du vote, ainsi que la sécurité et l'intégrité des échanges.



Que faire ?

Dans le cadre de la mise en œuvre d'élections par voie électronique, la CNIL recommande notamment[1] :

➢ l'expertise indépendante du système de vote afin de vérifier que le vote de l'électeur n'est pas modifié par le système, qu'il est bien pris en compte et qu'il est bien anonyme ;

➢ la séparation des données à caractère personnel des électeurs et des votes afin de garantir le secret du vote ;

➢ le chiffrement du bulletin de vote de manière ininterrompue du poste de l'électeur jusqu'au dépouillement de l'urne afin de s'assurer de l'intégrité du vote avant qu'il n'atteigne l'urne ;

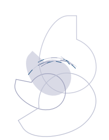
➢ le scellement du dispositif de vote afin de s'assurer qu'il n'est pas possible d'accéder aux bulletins contenus dans l'urne pendant le scrutin.

Il convient également d'informer les électeurs en temps utile par la remise d'une note explicative détaillant clairement les opérations de vote ainsi que le fonctionnement général du système de vote électronique.

Selon les cas, le dispositif de vote électronique peut relever :
- soit du régime de la demande d'avis auprès de la CNIL (A) ;
- soit du régime de la déclaration normale (B).

---

[1] Délibération de la CNIL n°03-036 du 1er juillet 2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électroniques



A - Le vote électronique est soumis à une demande d'avis dès lors qu'il s'agit d'un **téléservice de l'administration électronique[2],** c'est-à-dire qu'il remplit les caractéristiques suivantes :

➢ il est proposé par le biais d'un site internet ou sur des kiosques reliés à distance ;
➢ il nécessite l'utilisation d'un identifiant propre à chaque utilisateur ;
➢ il est proposé par l'administration ;
➢ il est à destination des usagers du service public.

Exemple

Une élection par voie électronique pour laquelle les étudiants sont les électeurs constitue un téléservice de l'administration électronique.

S'agissant plus particulièrement de l'élection aux conseils des universités, l'organisation de cette opération suppose le respect des dispositions du décret du 3 décembre 2004[3]. Seuls les étudiants peuvent être élus dans ces conditions, et seuls sont concernés le CA (Conseil d'Administration), le CS (Conseil Scientifique) et le CEVU (Conseil des Etudes et de la Vie Universitaire).

Les établissements autorisés à utiliser le vote électronique pour l'élection des représentants étudiants dans les trois conseils figurent sur une liste arrêtée par le ministre en charge de l'enseignement supérieur. A ce jour, seules deux universités y sont autorisées.

Attention !

Le dépôt d'un dossier de demande d'avis[4] auprès de la CNIL subsiste quand bien même un Correspondant Informatique et Libertés a été désigné et doit intervenir 2 mois minimum avant la mise en place effective du vote.

B - Lorsque le dispositif de vote électronique est strictement à destination des personnels de l'établissement, il relève alors du régime de la déclaration normale.

Exemple

Le vote par les personnels pour l'élection au conseil d'administration du CNRS, organisé selon les dispositions de l'arrêté du 29 mai 2008[5], est soumis au régime de déclaration normale.

---

2 En référence à l'article 27-II-4° de la loi « Informatique et Libertés ».

3 Décret n°2004-1326 du 3 décembre 2004 relatif au vote par voie électronique pour l'élection des représentants des usagers aux conseils des EPCSCP (Établissement Public à Caractère Scientifique, Culturel et Professionnel).

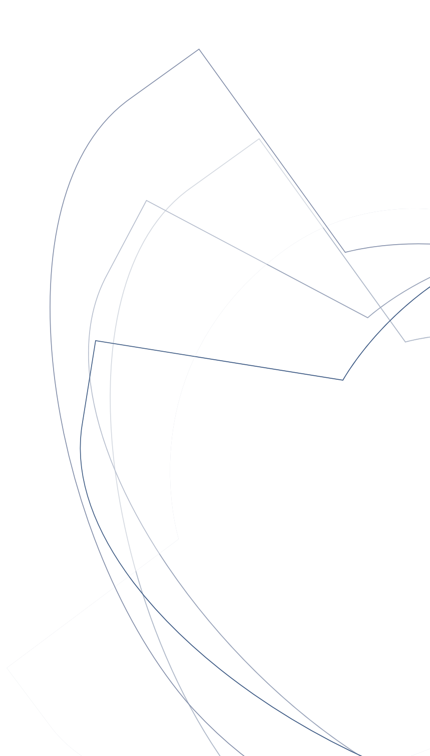
4 Le dossier de demande d'avis doit comporter l'annexe relative à la sécurité et le projet d'acte réglementaire (cf. modèle en annexe 3 du Guide).

5 Arrêté du 29 mai 2008 fixant les modalités d'élection au conseil d'administration du Centre national de la recherche scientifique.

En pratique

Si l'établissement a désigné un Correspondant Informatique et Libertés, ce dernier procèdera à la mise à jour du registre des traitements.
Sinon, une déclaration devra être effectuée auprès de la CNIL, précisant le nom du prestataire sélectionné ainsi que le descriptif technique précis du vote, de l'envoi des identifiants et mots de passe jusqu'au dépouillement de l'urne, **suffisamment** longtemps avant la mise en œuvre du traitement pour que le récépissé puisse être délivré avant la mise en œuvre du traitement

3 Annexes



Annexe 1 « Mode d'emploi : comment déclarer ? »

La déclaration est une obligation légale dont le non-respect est pénalement sanctionné[1]. Tout fichier ou traitement informatisé comportant des données personnelles doit donc être déclaré à la CNIL préalablement à sa mise en œuvre, sauf s'il est expressément exonéré de déclaration. Cette procédure de déclaration peut prendre plusieurs formes selon le fichier concerné[2].

Dans tous les cas, la désignation d'un Correspondant Informatique et Libertés dispense l'organisme concerné de l'accomplissement des formalités relatives aux fichiers relevant de la déclaration simplifiée et de la déclaration normale.

1 Les dispenses de déclaration

Un certain nombre de traitements, décrits dans le tableau récapitulatif figurant ci-après, sont dispensés de déclaration par une décision de la CNIL (ex. : site web institutionnel, sites web personnels).

Par ailleurs, les fichiers de gestion des étudiants et des personnels des établissements de l'enseignement supérieur n'ont pas en principe à être déclarés auprès de la CNIL dans la mesure où ils ont fait l'objet d'une déclaration par le Ministère de l'Éducation nationale (ex. : application APOGEE pour la gestion du fichier des étudiants, application GESUP pour la gestion des personnels des enseignants-chercheurs).

2 La déclaration normale

Le régime de droit commun est la **déclaration normale**, lorsque le fichier ne relève pas d'une procédure particulière (art. 22 de la loi "Informatique et Libertés"). Le traitement peut être mis en œuvre dès réception du récépissé délivré par la CNIL.

Le récépissé atteste de l'accomplissement des formalités de déclaration, mais n'exonère pas le responsable du traitement des autres obligations prévues par la loi (respect de la finalité du fichier, sécurité et confidentialité, respect des droits des personnes…).

3 La déclaration simplifiée

Certains des fichiers des établissements de l'enseignement supérieur et de la recherche peuvent faire l'objet de **déclarations simplifiées**.

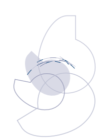
4 Les formalités particulières

Certains traitements des établissements d'enseignement peuvent relever d'un régime d'**autorisation** ou de **demande d'avis**. Il s'agit de régimes plus protecteurs, qui s'appliquent aux fichiers considérés comme « sensibles » ou comportant des risques pour la vie privée ou les libertés.

---

1 Article 226-16 du code pénal : « *Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende* ».

2 Le régime déclaratif des principaux fichiers mis en œuvre par les établissements de l'enseignement supérieur est indiqué dans le tableau récapitulatif figurant ci-après.



4.1 La procédure d'autorisation concerne (art. 25)

- les traitements qui comportent des données dites sensibles[3];
- les traitements qui comportent des données relatives aux infractions ou condamnations ;
- les traitements qui procèdent à l'interconnexion de fichiers dont les finalités correspondent à des intérêts publics différents ;
- les traitements de données comportant des appréciations sur les difficultés sociales des personnes Exemple : délibération n°2005-233 du 18 octobre 2005 portant autorisation unique de mise en œuvre par le centre national des œuvres universitaires et scolaires (CROUS) d'un traitement automatisé de données à caractère personnel ayant pour finalité la gestion des aides ponctuelles allouées aux étudiants dans le cadre de l'action sociale et le suivi statistique de l'activité de services sociaux des centres régionaux des œuvres universitaires et scolaires)[4].
- les traitements qui utilisent des données biométriques.

Le traitement devra respecter en tous points le cadre fixé par l'autorisation délivrée par la CNIL.

4.2 La procédure de demande d'avis (art. 27)

concerne principalement les traitements comportant le numéro de sécurité sociale (NIR) ou nécessitant une interrogation du répertoire national d'identification des personnes physiques (RNIPP), et les téléservices de l'administration électronique comportant un identifiant.

La demande d'avis doit être accompagnée d'un projet d'arrêté ou de décision de l'organe délibérant, destiné à autoriser le traitement une fois l'avis de la CNIL rendu.

5 Une fois le dossier complété

- dans le cas d'une télédéclaration, la CNIL adresse immédiatement après envoi un accusé de réception électronique[5] ;
- dans le cas d'une déclaration au moyen du formulaire papier, cette dernière doit être adressée par envoi recommandé avec demande d'avis de réception postal à la CNIL (8 rue Vivienne, CS 30223 75083, Paris Cedex 02) ou déposé auprès de la CNIL, contre reçu.

La CNIL délivre ensuite par voie postale ou électronique un **récépissé de déclaration** indiquant le numéro sous lequel le traitement déclaré est enregistré.

Pour les procédures particulières d'autorisation ou d'avis, la CNIL adresse au déclarant une notification de l'autorisation ou de l'avis qu'elle a rendu.

La plupart des formalités préalables peuvent être effectuées en ligne à partir du site web de la CNIL (www.cnil.fr).

---

3 Les données dites « sensibles » sont celles qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou la vie sexuelle des personnes (article 8 de la loi "Informatique et Libertés").

4 Toutefois, la CNIL n'applique pas la procédure d'autorisation pour les traitements destinés à gérer les demandes d'aides légales ou facultatives qui ne comportent pas l'évaluation de la situation sociale du demandeur conduite par un travailleur social et se limitent à l'enregistrement des données objectives nécessaires à l'attribution de l'aide en fonction de certains objectifs et de barèmes résultant de l'application des dispositions du code de l'action sociale et des familles.

5 Ne pas confondre l'accusé de réception d'un dossier de déclaration adressé à la CNIL avec le récépissé de déclaration délivré par la CNIL qui constitue le seul feu vert pour la mise en œuvre d'un fichier ou d'un traitement de données personnelles.

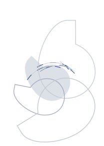
Tableau récapitulatif :
Dois-je déclarer mon fichier à la CNIL ? Comment ?

Rappel : les traitements n'ont pas à faire l'objet de déclaration[6] lorsqu'un Correspondant Informatique et Libertés a été désigné.

Déclarations à effectuer	Finalité des traitements
Pas de déclaration	➢ Gestion du fichier des étudiants (application APOGEE) (normalement déclaré par le Ministère de l'Éducation nationale arrêté du 26 janvier 1996) ➢ Gestion des personnels des enseignants-chercheurs (application GESUP) (déclaration du Ministère de l'Éducation nationale - arrêté du 6 juillet 1994) ➢ Les sites web vitrines ou institutionnels permettant par exemple l'envoi de lettre d'information. (à condition de respecter la dispense n°7) ➢ Les sites web personnels : sites diffusant ou collectant des données à caractère personnel mis en œuvre par des particuliers dans le cadre d'activités exclusivement personnelles tels que les « *blogs* ». (à condition de respecter la dispense n° 6)
Déclaration simplifiée	➢ Les sites web portail dans le cadre des espaces numériques de travail (ENT). Engagement de conformité à l'arrêté « ENT » du 30 novembre 2006 pris par le Ministère de l'Éducation nationale (acte réglementaire unique n° 003) ➢ Gestion des bourses par les centres régionaux des œuvres universitaires et scolaires (CROUS) (application nationale SAGA). Engagement de conformité avec l'autorisation unique n° 002 adoptée par la CNIL par une délibération n° 2005-233 du 18 octobre 2005
Déclaration normale	Gestion du fichier de médecine préventive[7]
Demande d'avis (Téléservice de l'administration électronique)	Les fichiers mis en œuvre dans le cadre d'opérations de vote électroniques (ex : élections des étudiants au sein du Conseil d'administration d'une université). (cf. recommandation n° 03-036 du ler juillet 2003 sur la sécurité des systèmes de vote électronique)
Autre Le principe est celui d'une déclaration normale mais il existe des exceptions. Pour les connaître, consulterle site de la CNIL.	Tout autre traitement automatisé, dès lors qu'il n'est pas conforme aux normes élaborées par la Commission, notamment : ➢ suivi de cohortes d'étudiants ➢ annuaire des anciens élèves ➢ gestion des stagiaires ➢ Junior entreprises ➢ vidéosurveillance ➢ sites internet (sauf ceux qui relèvent des dispenses) ➢ autres

6 Par contre les demandes d'autorisation ou d'avis à la CNIL subsistent.

7 En matière de données de santé, rappelons que celles-ci sont couvertes par le secret médical et dès lors, seuls les professionnels de santé peuvent y accéder. En aucun cas le responsable d'établissement ni même le Correspondant Informatique et Libertés ne sont habilités à obtenir communication de ces données.



Traitements statistiques (études, recherches)

Déclarations à effectuer	Finalité des traitements
Déclaration simplifiée	➢ Enquêtes par sondage intéressant des personnes physiques effectuées par l'État et les établissements publics à caractère administratif. (en référence à la norme simplifiée n° 19). ➢ Pour les recherches dans le domaine biomédical. (en référence à l'engagement de conformité à une méthodologie de référence n° MR-001).
Déclaration normale	➢ Suivi de cohortes. ➢ Traitement de données sensibles visées à l'article 8 de la loi "Informatique et Libertés" (ex. mesure de la diversité) : si consentement.
Demande d'autorisation	➢ Traitement de données sensibles visées à l'article 8 de la loi "Informatique et Libertés" (ex : mesure de la diversité) : si intérêt public ou anonymisation à bref délai. ➢ Recherches médicales menées en partenariat avec d'autres organismes (INSERM, CNRS). (pour les recherches dans le domaine de la santé (ex. recherches épidémiologiques).

CPU - AMUE - CNIL © 2009

Modèles de note d'information

Modèle de note d'information à porter sur les formulaires de collecte

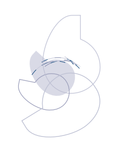
________________________________ (indication de l'identité du responsable du traitement)

« Les informations recueillies font l'objet d'un traitement informatique destiné à ... (*préciser la finalité. Les destinataires des données sont :* ________________ *(précisez*). Conformément à la loi "Informatique et Libertés", vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser à ________________________________ *(préciser le service).* [vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant] [1] »

Exemple de note d'information à utiliser sur le dossier d'inscription des étudiants

« Les informations recueillies par [*préciser ici l'identité du responsable du traitement* – en l'espèce l'université XX ou l'établissement XX] font l'objet d'un traitement informatique destiné à assurer la gestion administrative et pédagogique des étudiants, à établir des statistiques par le Ministère de l'éducation nationale et le rectorat et à permettre des enquêtes sur les conditions de vie des étudiants par l'Observatoire de la vie étudiante. Les organismes de sécurité sociale et les mutuelles étudiantes ainsi que le CROUS sont également destinataires d'informations nécessaires à l'accomplissement de leurs missions. Conformément à la loi "Informatique et Libertés", vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser à .... [*Préciser le service chargé du droit d'accès – en principe, il doit pouvoir s'exercer auprès du responsable d'établissement dans lequel l'étudiant est inscrit*]. »

1 À ne pas faire figurer si le traitement présente un caractère obligatoire.



Modèle de note d'information susceptible d'être affichée

« Le(s) service(s) ________________________________ (*citer le nom du ou des services concernés*) dispose(nt) de moyens informatiques destinés à gérer plus facilement __________________________ (*indiquer la finalité du traitement*).

Les informations enregistrées sont réservées à l'usage du (ou des) service(s) concerné(s) et ne peuvent être communiquées qu'aux destinataires suivants : ... (*préciser les destinataires*).

Conformément aux articles 39 et suivants de la loi "Informatique et Libertés", toute personne peut obtenir communication et, le cas échéant, rectification ou suppression des informations la concernant, en s'adressant au service _________ ___________________________ (*citer le nom du service ou des services concernés*). [toute personne peut également, pour des motifs légitimes, s'opposer au traitement des données la concernant] [2] »

2 À ne pas faire figurer si le traitement présente un caractère obligatoire.

CPU - AMUE - CNIL © 2009

Modèle de clause de confidentialité dans le cadre d'un marché ou d'un contrat de sous-traitance

Les supports informatiques fournis par l'établissement et tous documents de quelque nature qu'ils soient résultant de leur traitement par la société .... restent la propriété de l'établissement.

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226.13 du code pénal). Conformément à l'article 34 de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, la société .... s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

La société .... s'engage donc à respecter, de façon absolue, les obligations suivantes et à les faire respecter par son personnel, c'est-à-dire notamment à :

- ➢ ne prendre aucune copie des documents et supports d'informations confiés par la société .... et utilisés par la société .... à l'exception de celles nécessaires pour les besoins de l'exécution de sa prestation, objet du présent contrat ;
- ➢ ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat ;
- ➢ ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- ➢ prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;
- ➢ prendre toutes mesures, notamment de sécurité matérielle, pour assurer la conservation des documents et informations traités tout au long de la durée du présent contrat ;

et en fin de contrat à :

- ➢ procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies ;

ou à :

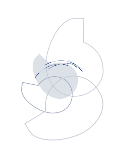
- ➢ restituer intégralement les supports d'informations selon les modalités prévues au présent contrat.

À ce titre, également, la société .... ne pourra sous-traiter l'exécution des prestations à une autre société, ni procéder à une cession de marché. Les supports d'informations qui lui seront remis devront être traités sur le territoire français métropolitain.

L'établissement se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par la société ....

Il est rappelé que, en cas de non-respect des dispositions précitées, la responsabilité du titulaire peut également être engagée sur la base des dispositions des articles 226-17 et 226-5 du code pénal.

L'établissement pourra prononcer la résiliation immédiate du contrat, sans indemnité en faveur du titulaire, en cas de violation du secret professionnel ou de non-respect des dispositions précitées.



Annexe 3 Modèle de projet d'acte réglementaire

En cas de demande d'avis auprès de la CNIL (ex. : pour la mise en place d'un téléservice de l'administration électronique), il convient de joindre au dossier de formalités déclaratives un projet d'acte réglementaire portant création du traitement. Il doit être adapté et complété en fonction des caractéristiques du traitement.

Projet de . …....…………..………… [1] relatif à l'informatisation de ……....………………… (préciser le service)

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, notamment ses articles 27 et 29 ;

Vu l'avis de la Commission Nationale de l'Informatique et des Libertés en date du xxx [2]

Arrête (ou décide)

Article 1 : il est créé par ……...……… un traitement automatisé de données à caractère personnel, dénommé ……........………….. dont l'objet est de ……...……………… (préciser la finalité).[3]

Article 2 : les catégories de données à caractère personnel enregistrées sont les suivantes : …………………………………………………………………………………………………

Article 3 : les destinataires ou catégories de destinataires habilités à recevoir communication de ces données sont, à raison de leurs attributions respectives :.......... ……………………………………………

Article 4 : le droit d'accès et de rectification prévu par les articles 39 et suivants de la loi n° 78-17 du 6 janvier 1978 s'exerce auprès du service ……………………………………………..

Article 5 (le cas échéant) [4] : le droit d'opposition prévu au titre de l'article 38 de la loi du 6 janvier 1978 ne s'applique pas au présent traitement.

Article 6 : le …………… [5] est chargé de l'exécution du présent ……………(préciser : arrêté, délibération, décision…) qui sera affiché en …………………et/ou publié au …………… [6]

---

1 Selon la nature juridique de l'organisme, l'acte réglementaire pourra prendre la forme suivante : décision du conseil d'administration, arrêté ministériel.

2 Ce visa devra être complété lors de la réception de l'avis de la CNIL, par la mention de la date figurant dans le courrier de la CNIL notifiant l'avis au déclarant.

3 Pour compléter les articles 1, 2 ,3 et 4, il convient de reprendre les informations indiquées dans le formulaire de déclaration.

4 Article à faire figurer dans la mesure où le traitement présente un caractère obligatoire.

5 Indiquer la fonction de la personne chargée de l'exécution de l'acte réglementaire.

6 Les actes réglementaires, quel qu'en soit l'auteur, sont soumis à la publication : celle-ci est la condition nécessaire à leur entrée en vigueur et, donc, à leur opposabilité. Le plus souvent, la publication consiste en une insertion de l'acte réglementaire dans un recueil officiel. Mais elle peut prendre d'autres formes (ex : affichage dans les locaux, diffusion sur le site internet de l'organisme, publication dans un journal spécialisé d'annonces légales, dans la presse locale…). L'avis de la CNIL devra également être publié.

CPU - AMUE - CNIL © 2009

Annexe 4 Les références législatives et réglementaires

Textes internationaux et européens

- Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à l'égard du traitement automatisé des données à caractère personnel

- Convention européenne de sauvegarde des Droits de l'Homme et des Libertés fondamentales de 1950

- Directive 95/46/CE du Parlement européen et du conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

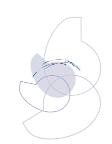
- Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection des la vie privée dans le secteur des télécommunications

Textes en droit français

- Loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés

- Décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

- Loi n°78-735 du 17 juillet 1978 modifiée portant diverses mesures d'amélioration des relations entre l'administration et le public (CADA)



Annexe 5 Lexique "Informatique et libertés"

CNIL

Autorité administrative indépendante, composée d'un collège pluraliste de 17 commissaires, provenant d'horizons divers (4 parlementaires, 2 membres du Conseil économique et social, 6 représentants des hautes juridictions, 5 personnalités qualifiées désignées par le président de l'Assemblée nationale (1), par le président du Sénat (1), par le conseil des ministres (3). Le mandat de ses membres est de 5 ans. Le président est élu par ses pairs.

Correspondant Informatique et Libertés

Créé en 2004, le correspondant informatique et libertés (CIL) est chargé d'assurer de manière indépendante le respect des obligations prévues par la loi "Informatique et Libertés" ; en contre-partie de sa désignation, les traitements de données personnelles les plus courants sont exonérés de déclarations auprès de la CNIL.

Destinataire

Personne habilitée à obtenir communication de données enregistrées dans un fichier ou un traitement en raison de ses fonctions.

Donnée biométrique

Caractéristique physique ou biologique permettant d'identifier une personne (ADN, contour de la main, empreintes digitales…).

Donnée personnelle

Toute information identifiant directement ou indirectement une personne physique (ex. nom, n° d'immatriculation, n° de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale.....).

Donnée sensible

Information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.

Droit à la protection des données personnelles

Le droit à la protection des données à caractère personnel est inscrit dans la charte des droits fondamentaux de l'Union européenne au titre des libertés fondamentales telles que la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information ou le respect de la vie privée et familiale, etc.

CPU - AMUE - CNIL © 2009

Droit à l'information

Toute personne a un droit de regard sur ses propres données ; par conséquent, quiconque met en œuvre un fichier ou un traitement de données personnelles est obligé d'informer les personnes fichées de son identité, de l'objectif de la collecte d'informations et de son caractère obligatoire ou facultatif, des destinataires des informations, des droits reconnus à la personne, des éventuels transferts de données vers un pays hors de l'Union Européenne.

Droit d'accès direct

Toute personne peut prendre connaissance de l'intégralité des données la concernant dans un fichier en s'adressant directement à ceux qui les détiennent, et en obtenir une copie dont le coût ne peut dépasser celui de la reproduction.

Droit d'accès indirect

Toute personne peut demander que la CNIL vérifie les renseignements qui peuvent la concerner dans les fichiers intéressant la sûreté de l'État, la Défense et la Sécurité publique.

Droit d'opposition

Toute personne a la possibilité de s'opposer, pour des motifs légitimes, à figurer dans un fichier, et peut refuser sans avoir à se justifier, que les données qui la concernent soient utilisées à des fins de prospection, notamment, commerciale.

Droit de rectification

Toute personne peut faire rectifier, compléter, actualiser, verrouiller ou effacer des informations la concernant lorsqu'ont été décelées des erreurs, des inexactitudes ou la présence de données dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Fichier des fichiers

Liste des fichiers déclarés à la CNIL, ainsi que leurs caractéristiques.

Finalité d'un traitement

Objectif principal d'une application informatique de données personnelles. Exemples de finalité : gestion des recrutements, gestion des clients, enquête de satisfaction, surveillance des locaux, etc.

Formalités préalables

Ensemble des formalités déclaratives à effectuer auprès de la CNIL avant la mise en œuvre d'un traitement de données personnelles ; selon les cas, il peut s'agir d'une déclaration ou d'une demande d'autorisation.



Formation restreinte

Pour prendre des mesures à l'encontre des responsables de traitement qui ne respectent pas la loi informatique et libertés, la CNIL siège dans une formation spécifique, composée de six membres appelée "formation restreinte". À l'issue d'une procédure contradictoire, cette formation peut notamment décider de prononcer des sanctions pécuniaires pouvant atteindre 300 000 €.

Listes d'opposition

Les listes d'opposition recensent les personnes qui ont fait connaître leur opposition à être prospectées dans le cadre d'opérations de marketing.

NIR

Le Numéro d'Inscription au Répertoire ou numéro de sécurité sociale est attribué à chaque personne à sa naissance sur la base d'éléments d'état civil transmis par les mairies à l'INSEE.

Responsable du traitement

Personne qui décide de la création d'un fichier ou d'un traitement de données personnelles, qui détermine à quoi il va servir et selon quelles modalités.

Séance plénière

C'est la formation qui réunit les 17 membres de la CNIL pour se prononcer sur des traitements ou des fichiers et examiner des projets de loi ou de décrets soumis pour avis par le Gouvernement.

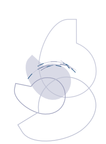
Traitement de données

Collecte, enregistrement, utilisation, transmission ou communication d'informations personnelles, ainsi que toute exploitation de fichiers ou bases de données, notamment des interconnexions.

Transfert de données

Toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne.

CPU - AMUE - CNIL © 2009



Remerciements

Cet outil a été réalisé grâce au concours du groupe projet « guide Informatique et Libertés » et nous les en remercions tout particulièrement.

Les Correspondants Informatique et Libertés universitaires

- Guy BISIAUX, ingénieur réseau système, CIL de l'université Valenciennes et du Hainaut-Cambresis
- Solenn HOUSSAY, chargée de la sécurité des systèmes d'information, CIL de l'université de Lyon 3 - Jean Moulin
- Myriam RAVALET-GUILLET, responsable des affaires juridiques, CIL de l'université de Rennes 1
- Claire RUBAT du MERAC, coordination de la sécurité des systèmes d'information, CIL mutualisée pour les universités de Grenoble 1 - Joseph Fourier, Grenoble 2 - Pierre Mendès France, Grenoble 3-Stendhal, l'INP de Grenoble et l'université de Savoie - Chambéry
- Yves SENDRA, responsable de la sécurité des systèmes d'information, CIL de l'université de Nice-Sophia-Antipolis
- Jean-Luc TESSIER, responsable du service informatique des services centraux, CIL de l'université de Lille 2
- Thierry VALET, professeur agrégé économie-gestion, CIL de l'université d'Avignon

Comité Réseaux des Universités (CRU)

- Serge AUMONT, membre du Comité
- Roger NEGARET, responsable de la sécurité des systèmes d'information, université de Rennes 1[1]

---

1 Au titre de sa contribution au document « Politique type de gestion des journaux informatiques » porté par le CRU, mentionné à la fiche n°13.

CPU - AMUE - CNIL © 2009

Agence de mutualisation des universités et établissements (Amue)

- Simon LARGER, chargé de domaine finances, département Services

Commission Nationale de l'Informatique et des Libertés (CNIL)

- Marie GEORGES, conseiller du président pour la prospective et le développement
- Leslie BASSE, juriste auprès de la direction des affaires juridiques, internationales et de l'expertise

Conférence des Présidents d'Université (CPU)

- Florence BENOIT-ROHMER, présidente de la commission du règlement et de la législation et de l'université Robert Schuman-Strasbourg 3
- Claire SOURBÈS, chargée de mission auprès de la commission du règlement et de la législation